**Security Guide**
Document version: 2.2 – 2015-12-11

**CUSTOMER**

# SAP Customer Activity Repository 2.0 FP2

# Typographic Conventions

Table 1

| Example | Description |
| --- | --- |
| **<Example>** | Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, "Enter your **<User Name>**". |
| *Example* > *Example* | Arrows separating the parts of a navigation path, for example, menu options |
| **Example** | Emphasized words or expressions |
| **Example** | Words or characters that you enter in the system exactly as they appear in the documentation |
| www.sap.com | Textual cross-references to an internet address |
| /example | Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web |
| 123456 | Hyperlink to an SAP Note, for example, SAP Note 123456 |
| *Example* | • Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options.<br>• Cross-references to other documentation or published works |
| `Example` | • Output on the screen following a user action, for example, messages<br>• Source code or syntax quoted directly from a program<br>• File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools |
| `EXAMPLE` | Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, `SELECT` and `INCLUDE` |
| EXAMPLE | Keys on the keyboard |

# Content

# 1 Introduction

> **Caution**
> This guide does not replace the daily operations handbook that we recommend customers create for their specific productive operations.

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereby the Security Guides provide information that is relevant for all life cycle phases.

### Why is Security Necessary

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to the SAP Customer Activity Repository. To assist you in securing the SAP Customer Activity Repository, we provide this Security Guide.

### About This Document

The Security Guide provides an overview of the security-relevant information that applies to the SAP Customer Activity Repository.

#### Overview of the Main Sections

The Security Guide comprises the following main sections:

- Before You Start

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.
- Technical System Landscape

  This section provides an overview of the technical components and communication paths that are used by SAP Customer Activity Repository.
- Security Aspects of Data, Data Flow and Processes

  This section provides an overview of security aspects involved throughout the most widely-used processes within SAP Customer Activity Repository.
- User Administration and Authentication

  This section provides an overview of the following user administration and authentication aspects:
  - Recommended tools to use for user management.
  - User types that are required by SAP Customer Activity Repository.
  - Standard users that are delivered with SAP Customer Activity Repository.
  - Overview of the user synchronization strategy, if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.
- Authorizations

This section provides an overview of the authorization concept that applies to SAP Customer Activity Repository.

- Session Security Protection

  This section provides information about activating secure session management, which prevents JavaScript or plug-ins from accessing the SAP logon ticket or security session cookie(s).

- Network and Communication Security

  This section provides an overview of the communication paths used by SAP Customer Activity Repository and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- Internet Communication Framework Security

  This section provides an overview of the Internet Communication Framework (ICF) services that are used by SAP Customer Activity Repository.

- Data Storage Security

  This section provides an overview of any critical data that is used by SAP Customer Activity Repository and the security mechanisms that apply.

- Data Protection

  This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements related to data privacy.

- Security for Third-Party or Additional Applications

  This section provides security information that applies to third-party or additional applications that are used with SAP Customer Activity Repository.

- Enterprise Services Security

  This section provides an overview of the security aspects that apply to the enterprise services delivered with SAP Customer Activity Repository.

- Security-Relevant Logging and Tracing

  This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- Services for Security Lifecycle Management

  This section provides an overview of services provided by Active Global Support that are available to assist you in maintaining security in your SAP systems on an ongoing basis.

- Reference

  This section provides references to further information.

# 2 Before You Start

## Fundamental Security Guides

SAP Customer Activity Repository is built on the SAP NetWeaver Application Server ABAP and is implemented on the SAP HANA database. Therefore, the corresponding Security Guides also apply to SAP Customer Activity Repository.

Table 2: Fundamental Security Guides

| Scenario, Application, or Component Security Guide | Most-Relevant Sections or Specific Restrictions |
|---|---|
| SAP HANA Security Guide | help.sap.com/hana/ ▶ *SAP HANA Appliance Software* ▶ *Security Information* ▶ *SAP HANA Security Guide* |
| *Security* section of the Administrator's Guide, SAP HANA Live for SAP Business Suite | help.sap.com/hba ▶ *Master, Installation, Security, Configuration, and Operations Information* ▶ *Administrator's Guide* |
| SAP NetWeaver 7.4 Security Guide | help.sap.com/nw74/ ▶ *Security Information* ▶ *Security Guide* |
| Portal Security Guide | help.sap.com/nw74/ ▶ *Security Information* ▶ *Security Guide* ▶ *Security Guides for SAP NetWeaver Functional Units* ▶ *Enterprise Portal (EP) and EP Core* ▶ *Portal Security Guide* |
| SAP NetWeaver Application Server ABAP Security Guide | help.sap.com/nw74/ ▶ *Security Information* ▶ *Security Guide* ▶ *Security Guides for SAP NetWeaver Functional Units* ▶ *Security Guides for the Application Server* ▶ *Security Guides for AS ABAP* ▶ *SAP NetWeaver Application Server ABAP Security Guide* |
| Security Guide for SAP NetWeaver BW | help.sap.com/nwbw/ ▶ *<Your SAP NetWeaver Business Warehouse version>* ▶ *Security Information* ▶ *Security Guide* ▶ *Security Guides for SAP NetWeaver Functional Units* ▶ *Security Guide for SAP NetWeaver BW* |
| SAP ERP 6.0 EHP 5 Security Guide | help.sap.com/erp/ ▶ *Security Information* ▶ *SAP Service MarketPlace* ▶ *6.0, EHP5* ▶ *SAP ERP Central Component: Security Guide* |
| SAP for Retail (Industry Solution) | help.sap.com/retail-erp605/ ▶ *Security Information* ▶ *SAP Service MarketPlace* ▶ *SAP Security Guides* ▶ *Industry Solutions* ▶ *SAP for Retail* ▶ *SAP for Retail* ▶ *Security Guide – SAP for Retail* |
| SAP Smart Business Products Administrator's Guide | help.sap.com/ssb/ ▶ *Installation, Security, Configuration, and Operations Information* ▶ *Administrator's Guide* |

For a complete list of the available SAP Security Guides, see service.sap.com/securityguide on the SAP Service Marketplace.

## Important SAP Notes

The most important SAP Notes that apply to the security of the SAP Customer Activity Repository application are shown in the table below.

Table 3: Important SAP Notes

| Title | SAP Note Number | Comment |
|---|---|---|
| SAP HANA 1.0: Security | 159623 | Contains information and links to other notes related to the secure operation of SAP HANA. |
| Key replacement for encryption of payment card data | 1151936 | Contains information about functions for a periodic key replacement for the encryption of payment card data. |
| Credit card encryption in the POS Data Management | 1053296 | Contains information on using credit card encryption. |
| Credit card coding in ERP POS inbound | 1041514 | Contains information on adjustments for the coding of credit card information in POS inbound. |
| Secure handling of credit card data in ERP | 1032588 | Contains information on enabling secure handing of credit card data in ERP. |
| LPA: Settings for enabling Transaction Viewer | 1533599 | Contains information on the settings necessary to support LPA services used by the SAP NetWeaver Portal. |
| Authorization Check for Function Modules in SAP Customer Activity Repository and SAP POS DM | 1940161 | Contains information about authorization objects required to support integration scenarios involving systems connected to SAP Customer Activity Repository using RFC connections. |

For a list of additional security-relevant SAP Hot News and SAP Notes, see also SAP Service Marketplace at service.sap.com/securitynotes.

## Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

Table 4: Quick Links to Additional Information

| Content | Quick Link on the SAP Service Marketplace or SDN |
|---|---|
| Security | sdn.sap.com/irj/sdn/security |
| Security Guides | service.sap.com/securityguide |
| Related SAP Notes | support.sap.com/notes |

| Content | Quick Link on the SAP Service Marketplace or SDN |
| --- | --- |
| | support.sap.com/securitynotes |
| Released Platforms | support.sap.com/pam |
| SAP Solution Manager | support.sap.com/solutionmanager |
| SAP NetWeaver | sdn.sap.com/irj/sdn/netweaver |

# 3 Technical System Landscape

The figure below shows an overview of the technical system landscape for the SAP Customer Activity Repository application.

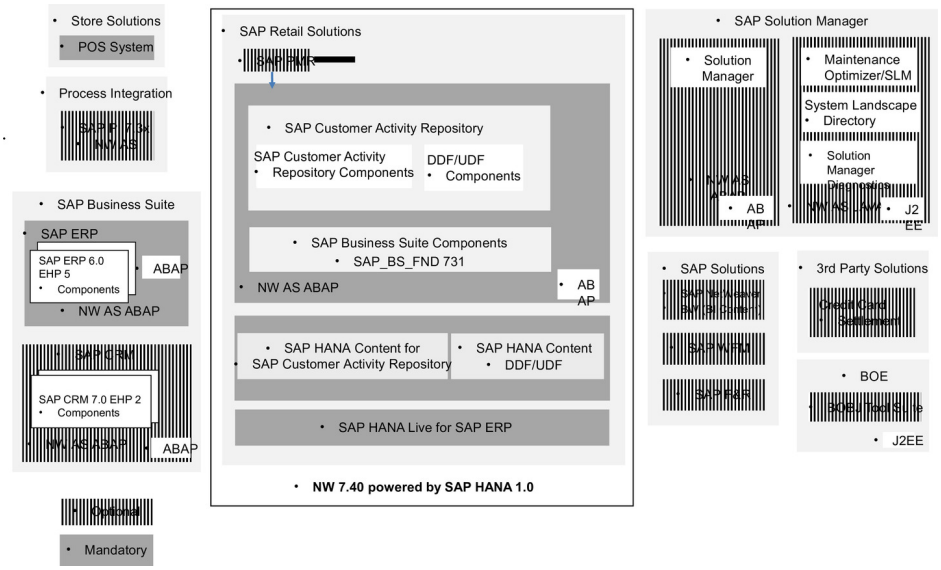



Figure 1: Technical System Landscape

For more information about the technical system landscape, see the resources listed in the table below.

Table 5: More Information About the Technical System Landscape

| Topic | Guide/Tool | Quick Link to the SAP Service Marketplace or SDN |
|---|---|---|
| Technical description for the SAP Customer Activity Repository application and the underlying technological components such as SAP NetWeaver. | *Master Guide* | service.sap.com/instguides |
| High availability | *High Availability for SAP Solutions* | sdn.sap.com/irj/sdn/ha |
| Technical landscape design | See applicable documents | sdn.sap.com/irj/sdn/landscapedesign |
| Security | See applicable documents | service.sap.com/security |

# 4 Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the data flow process for the SAP Customer Activity Repository application.

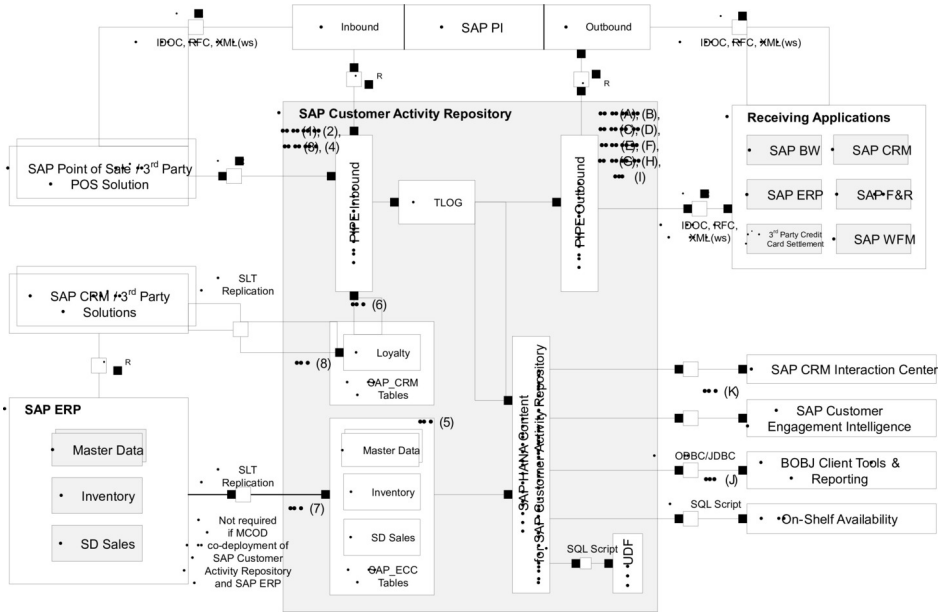



Figure 2: SAP Customer Activity Repository Data Flow Process

The table below shows the security aspect to be considered for the process step and what mechanism applies.

Table 6

| Step | Description | Security Measure |
|---|---|---|
| Inbound Flow 1 | Manual creation of transaction within POS Workbench (ABAP DynPro / Web DynPro) | SAP Dialog User with necessary authorizations |
| Inbound Flow 2 | Inbound transaction from SAP Retail using IDoc | SAP Communication User with necessary authorizations, ALE tRFC, encryption** |
| Inbound Flow 3 | Inbound transaction using BAPI | SAP Communication User with necessary authorizations, RFC |
| Inbound Flow 4 | Inbound transaction using Web Service | SAP Communication User with necessary authorizations, HTTPS |
| Inbound Flow 5 | Master data retrieval (non-sensitive data) | SAP Dialog/Communication User with necessary authorizations, RFC |

| Step | Description | Security Measure |
| --- | --- | --- |
| Inbound Flow 6 | Loyalty card data retrieval from a CRM solution (non- sensitive data) | SAP Dialog/Communication User with necessary authorizations, RFC |
| Inbound Flow 7 (when required) | Data replication from SAP ERP.<br>**Note**<br>Replication is not required in cases of Multiple Components in One Database (MCOD) co-deployment of SAP Customer Activity Repository and SAP ERP.<br>For more information, see<br>help.sap.com/car > *Installation and Upgrade Information* > *Installation Guide*. | SLT replication (SAP system user with necessary authorizations to set up replication, SAP technical user(s) with necessary authorizations for replication of target schema) |
| Inbound Flow 8 | Loyalty data replication from a CRM solution | SLT replication (SAP system user with necessary authorizations to set up replication, SAP technical user(s) with necessary authorizations for replication of target schema |
| Outbound Flow A* | Outbound Aggregated Sales to SAP Retail using IDoc | SAP Communication User with necessary authorizations, ALE tRFC, encryption** |
| Outbound Flow B* | Outbound Sales Data & Goods Receipt/ Issue Information to SAP F&R using BAPI | SAP Communication User with necessary authorizations, RFC |
| Outbound Flow C* | Outbound Credit Card Settlement using BAPI | SAP Communication User with necessary authorizations, RFC |
| Outbound Flow D* | Outbound Payment Card using BAPI | SAP Communication User with necessary authorizations, RFC |
| Outbound Flow E* | Outbound Inventory Management / Goods Movement to SAP ERP using BAPI | SAP Communication User with necessary authorizations, RFC |
| Outbound Flow F* | Outbound (Aggregated) Sales Data to DMF using BAPI | SAP Communication User with necessary authorizations, RFC |
| Outbound Flow G* | Outbound Loyalty Information using Web Service | SAP Communication User with necessary authorizations, HTTPS |
| Outbound Flow H* | Outbound Sales Analysis, Error Statistics, and Loss Prevention Information to SAP BI | SAP Dialog/Communication User with necessary authorizations |

| Step | Description | Security Measure |
| --- | --- | --- |
| Outbound Flow I* | Outbound Aggregated Historical Transaction & Product Sales Counts to SAP WFM using IDoc | SAP Communication User with necessary authorizations, ALE tRFC |
| Outbound Flow J | Analytical query view data (for example, Inventory Visibility, and so on) to reporting tools | SAP Hana Database User with necessary object & analytical privileges, ODBC/JDBC |
| Outbound Flow K | Customer-based view data (for example, customer segmentation, and so on) to SAP CRM | SAP Communication User with necessary authorizations, RFC |

* Within Task Processing

** Sensitive data that must be encrypted would consist of credit card information, and this information will be stored in a secure manner within the SAP Customer Activity Repository database (for example, encrypted, masked, and so on).

# 5 User Administration and Authentication

SAP Customer Activity Repository uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the AS ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to SAP Customer Activity Repository.

The SAP HANA content for Customer Activity Repository uses the user management and authentication mechanisms provided with the SAP HANA appliance software. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *Security* section of the *Administrator's Guide, SAP HANA Live for SAP Business Suite, Support Package Stack 02* apply.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP Customer Activity Repository in the following topics:

- User Management

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the application.
- User Data Synchronization

  The application can share user data. This topic describes how the user data is synchronized with these other sources.
- Integration Into Single Sign-On Environments

  This topic describes how the application supports Single Sign-On mechanisms.

## 5.1 User Management

User management for SAP Customer Activity Repository uses the mechanisms provided by the SAP NetWeaver AS ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for the SAP Customer Activity Repository, see the sections below. In addition, we provide a list of the standard users required for operating SAP Customer Activity Repository.

Similarly, other components of the technical system landscape for SAP Customer Activity Repository, such as SAP ERP Central Component (ECC) and/or SAP NetWeaver Process Integration (PI), also use the mechanisms provided with the SAP NetWeaver AS ABAP.

### User Administration Tools

The table below shows the tools to use for user management and user administration with SAP Customer Activity Repository.

Table 7: User Management Tools

| Tool | Description | Requirements |
|---|---|---|
| User and role maintenance with SAP NetWeaver AS ABAP (Transactions **SU01**, **PFCG**) | For more information, see: | SAP NetWeaver Application Server ABAP should be running. |

| Tool | Description | Requirements |
| --- | --- | --- |
| | • *AS ABAP Authorization Concept* in the *SAP NetWeaver Application Server ABAP Security Guide*<br>• SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw74 › *Application Help* › *Function-Oriented View* › *Solution Life Cycle Management* › *Security and User Administration* | |

### User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The user types that are required for the SAP Customer Activity Repository application include:

- Individual users:
  - Dialog users are used for interactive system access, such as SAP GUI for Windows or RFC connections.
  - Internet users are used for internet connections. The same policies apply as for dialog users, but used for Internet connections.
  - Named users are required for all Business Intelligence clients like SAP BusinessObjects BI Suite UIs.
- Technical users:
  - Communication users are used for dialog-free communication through external RFC calls.
  - Background users are used for background processing and communication within the system, such as, running scheduled inbound/outbound dispatcher jobs.

For more information on these user types, see *User Types* in the *SAP NetWeaver Application Server ABAP Security Guide*.

All user types described in the *SAP HANA Security Guide* are required for the SAP HANA content for SAP Customer Activity Repository. For more information, see *User Types* in the *SAP HANA Security Guide*.

### Standard Users

SAP Customer Activity Repository does not require specialized standard users. The POS Data Transfer and Audit component of SAP Customer Activity Repository indirectly uses SAP NetWeaver standard users.

For more information about SAP NetWeaver standard users, see *Protecting Standard Users* in the *SAP NetWeaver Application Server ABAP Security Guide*.

> **Recommendation**
>
> We recommend changing the user IDs and passwords for any users that are automatically created during installation.

### Users and Roles for SAP Smart Business Applications

For more information on the users and roles required by specific SAP Smart Business applications delivered with SAP Customer Activity Repository, see SAP Help Portal at help.sap.com/car › *<your release>* › *Application*

*Help* > *Additional Content* > *SAP Smart Business for SAP Customer Activity Repository* > *SAP Smart Business for Multichannel Sales Analytics*. The *App Implementation* documentation for each SAP Smart Business application contains the information on the required users and roles.

### Users and Roles for Standalone SAP Fiori Apps

SAP Customer Activity Repository is delivered with the *Analyze Forecast* standalone app. For more information on the users and roles required by this app, see SAP Help Portal at help.sap.com/car > *<your release>* > *Application Help* > *Additional Content* > *Standalone SAP Fiori Apps for SAP Customer Activity Repository* > *Analyze Forecast* > *App Implementation: Analyze Forecast*.

## 5.2 User Data Synchronization

The application does not deliver additional user data synchronization related features in addition to those available in the SAP NetWeaver platform. It also does not impose any special needs or restrictions, which would limit the usage of related NetWeaver tools.

> **Recommendation**
>
> For any scenarios where system inter-connectedness at the user level is a requirement, it is recommended that the same users exist throughout all the pertinent connected systems in the landscape.

## 5.3 Integration Into Single Sign-On Environments

The SAP Customer Activity Repository supports the Single Sign-On (SSO) mechanisms provided by the SAP NetWeaver AS ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Security Guide* also apply to the SAP Customer Activity Repository application.

For more information about the available authentication mechanisms, see *User Authentication and Single Sign-On* in the *SAP NetWeaver Library*.

# 6 Authorizations

SAP Customer Activity Repository uses the authorization provided by the SAP NetWeaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide* also apply to the SAP Customer Activity Repository application.

The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction **PFCG**) on the AS ABAP.

> **Note**
>
> For more information about how to create roles, see *Role Administration* in the *SAP NetWeaver Library*.

## SAP HANA Content for SAP Customer Activity Repository

The SAP HANA content for SAP Customer Activity Repository relies on the access control mechanisms of the underlying SAP HANA database. As a prerequisite, it is assumed that every business user (user accessing SAP HANA content for SAP Customer Activity Repository in the SAP HANA database) is created as a named SAP HANA database user. To control the business user's access to the SAP HANA content and displayed data for SAP Customer Activity Repository, the relevant authorization settings must be configured in the SAP HANA database.

SAP HANA has implemented the regular SQL authorization concept based on privileges. For more information, see *Security* > *Authorizations* > *Privileges* in the *Administrator's Guide, SAP HANA Live for SAP Business Suite, Support Package Stack 02*.

## Analytics Authorization Assistant

The SAP HANA content for SAP Customer Activity Repository relies on a number of views from SAP HANA Live for SAP ERP. As a result we recommend that you use the Analytics Authorization Assistant to manage authorizations.

Analytics Authorization Assistant automatically locates authorizations that a user has in SAP NetWeaver AS ABAP and transforms these authorizations into analytic privileges on the SAP HANA database. The created analytic privileges are used to access applicable views included in SAP HANA Live for SAP ERP and SAP HANA content for SAP Customer Activity Repository. The analytical privileges are then assigned to SAP HANA roles and/or directly to users.

The user-specific authorizations required by SAP Customer Activity Repository, specifically, the data found in tables `USRBF2` and `UST12`, are maintained in a source SAP ERP system. Depending on the deployment option you have selected during the installation of SAP Customer Activity Repository, Analytics Authorization Assistant accesses authorization tables as follows:

Table 8

| Deployment Option | Table Access |
|---|---|
| SAP Customer Activity Repository co-deployed with SAP ERP | Directly from the SAP ERP database schema (`SAP_ECC`) on the SAP HANA database |
| SAP Customer Activity Repository standalone | From tables replicated to a dedicated SAP Customer Activity Repository schema from the source SAP ERP system |

The query views available as part of the SAP HANA content for SAP Customer Activity Repository rely on the following SAP ERP authorization objects, where applicable:

- `M_IS_WERKS` (Plant)
- `M_IS_VTWEG` (Distribution Channel)
- `M_IS_VKORG` (Sales Organization)
- `M_IS_MAKTL` (Material Group)

For more information about the Analytics Authorization Assistant in general, refer to SAP Note 1796718 and SAP Help Portal under help.sap.com/hba > *SAP HANA Live Tools* > *SAP HANA Live Authorization Assistant*.

### Authorizations to Support Integration Scenarios

SAP Customer Activity Repository supports the following integration scenarios:

- Loss Prevention Analytics (LPA) (task *5001*, SAP Standard Profile)
- Demand Management Foundation (DMF) sales reporting, provided through task processing (task *0050*, SAP Standard Profile)
- Inventory Management (IM) goods movement reporting to ERP, provided through task processing (task *0017*, SAP Standard Profile)
- Forecasting & Replenishment (F&R) sales reporting, provided through task processing (task *0020*, SAP Standard Profile)
- Credit Card Settlement, provided through task processing (task *0015*, SAP Standard Profile)
- Oil & Gas SSR Payment Card data processing in ERP, provided through task processing (task *0101*, SAP Standard Profile)

To enable these integration scenarios, the SAP Activity Repository system communicates with other SAP systems using Remote Function Calls (RFCs). The authorization objects that are verified during this integration are listed in SAP Note 1940161.

### Role and Authorization Concept for SAP Customer Activity Repository

The tables in the sections below show the standard roles and authorization objects that are used in the components of SAP Customer Activity Repository.

### Standard Roles for SAP Customer Activity Repository

The table below shows the standard roles that are used by SAP Customer Activity Repository.

Table 9: Standard Roles

| Role | Description |
|---|---|
| `/POSDW/ADMINISTRATOR` | Performs administrative activities that should not be executed by normal users. These include deleting data and explicitly reconstructing index records.<br>• Cross-application Authorization Objects (AAAB):<br>  ○ Transaction Code Check at Transaction Start<br>  S_TCODE field TCD has values:<br>  /POSDW/DELE, /POSDW/IDIS, /POSDW/IMG, /POSDW/ODIS, /POSDW/PDIS, /POSDW/QDIS, /POSDW/QMON, /POSDW/REFI, /POSDW/REFQ, /POSDW/REFT<br>• Basis: Administration (BC_A): |

| Role | Description |
| --- | --- |
| | ○ Cross Client Table Maintenance<br>S_TABU_CLI field CLII has value: ‚X' - Allowed: Maintenance of cross-client tables<br>○ Table Maintenance (via standard tools such as SM30)<br>S_TABU_DIS field ACTVT has values: 02 - Change 03 - Display<br>• Basis - Central Functions (BC_Z):<br>○ ALV Standard Layout<br>S_ALV_LAYO field ACTVT has value: 23 - Maintain<br>• SAP Point-Of-Sale Data Management (POSDM) (PIPE):<br>○ Authorizations for Outbound Processing in PIPE<br>W_POS_AGGP field /POSDW/OAC has value: 16<br>○ Authorizations for Aggregation in PIPE<br>W_POS_AGGR field /POSDW/AAC has values: 01, 02<br>○ Authorizations for PIPE-related tasks<br>W_POS_STAT field /POSDW/SAC has value: 01<br>○ Authorizations for Data on POS Transactions<br>W_POS_TRAN field /POSDW/PAC has values: 01, 03, 06, 24, 31, 32, 34 |
| /POSDW/SALES_AUDIT | Performs the daily monitoring of the POS inbound data, including analyses and evaluations.<br>• Cross-application Authorization Objects (AAAB):<br>○ Transaction Code Check at Transaction Start<br>S_TCODE field TCD has values: /POSDW/IDIS, /POSDW/MON0, /POSDW/MON1, /POSDW/MON2, /POSDW/PDIS<br>• SAP Point-Of-Sale Data Management (POSDM) (PIPE):<br>○ Authorizations for credit card numbers in PIPE<br>W_POS_CCNR fields have value: *<br>○ Authorizations for PIPE-related tasks<br>W_POS_STAT fields have value: *<br>○ Authorizations for Data on POS Transactions<br>W_POS_TRAN field /POSDW/PAC has values: 01, 02, 03 |
| /POSDW/SAP_QUERY_TRAN_S_RFC | Role with RFC authorization for query of POS transactions. This role contains all authorizations that are necessary to query POS transactions via the RFC module /POSDW/SALES_QUERY_RFC. It also contains all authorizations that are necessary to post the processing confirmation via the RFC module /POSDW/CONFIRM_AGGR_PACKS_ARFC.<br>• Basis and Administration (BC_A):<br>○ Auth. Check for RFC access<br>S_TCODE field:<br>○ ACTVT has value: 16 - Execute |

| Role | Description |
| --- | --- |
| | ○ RFC_NAME has values: /POSDW/CONFIRM_AGGR_PACK, /POSDW/SALES_QUERY_API, ARFC, ERFC<br>○ RFC_TYPE has value: FUGR |
| SAP_ISR_DDF_MASTER | First PFCG role required for the Demand Data Foundation (DDF) module in SAP Customer Activity Repository. The role grants access to the following DDF objects and services on the SAP Easy Access screen:<br>• Check Mass Maintenance<br>• Configure Load Balancing<br>• Define Area of Responsibility<br>• Location Groups<br>• Monitor Compressed Data<br>• Maintain Product Locations<br>• Monitor Exceptions<br>• Monitor Imports<br>• Placeholder Products<br>• Product<br>• Product Groups<br>• Remove Time Series<br>• Schedule Model and Forecasts<br>• Search for Schedule Jobs<br>• Search Placeholder Products<br>• Transportation Lanes |
| SAP_ISR_DDF_READONLY_MASTER | Second PFCG role required for the DDF module in SAP Customer Activity Repository. The role grants access to the following DDF objects and services on the SAP Easy Access screen:<br>• Check Mass Maintenance<br>• Configure Load Balancing<br>• Define Area of Responsibility<br>• Location Groups<br>• Maintain Product Locations<br>• Monitor Compressed Data<br>• Monitor Exceptions<br>• Monitor Imports<br>• Placeholder Products<br>• Product<br>• Product Groups<br>• Remove Time Series<br>• Schedule Model and Forecasts<br>• Search for Schedule Jobs<br>• Search Placeholder Products |

| Role | Description |
| --- | --- |
| | • Transportation Lanes |

## Standard Roles for On-Shelf Availability

The table below shows the standard roles that are used by the On-Shelf Availability (OSA) functionality in SAP Customer Activity Repository. These roles are required in addition to the technical role for SAP NetWeaver Gateway.

Table 10: Standard Roles

| Role | Description | Authorization Objects/Fields |
| --- | --- | --- |
| /OSA/MANAGER | Permissions assigned to a store manager who logs on. | • /OSA/STOR:OSA/STORE, ACTVT<br>• /OSA/DEPT:OSA/AREA, OSA/STORE, ACTVT<br>• /OSA/PROD:OSA/AREA, OSA/STORE, ACTVT |
| /OSA/EMPLOYEE | Permissions assigned to a store employee who logs on. | • /OSA/STOR:OSA/STORE, ACTVT<br>• /OSA/DEPT:OSA/AREA, OSA/STORE, ACTVT<br>• /OSA/PROD:OSA/AREA, OSA/STORE, ACTVT |
| /OSA/ADMINISTRATOR | Permissions for administrative activities:<br>• Dispatching of the OSA algorithm<br>• Archiving the status log data | • /OSA/ADM: /OSA/ADM_A |

## External Roles Specific to Loss Prevention Analytics

The table below shows the **external** roles, that is, roles defined outside of the SAP Customer Activity Repository application, that are only used if you are implementing the Loss Prevention Analytics functionality.

For more information on integrating SAP Customer Activity Repository with the existing Loss Prevention Analytics (LPA) business process of the Store Analytics business scenario, see SAP Note 2010774.

Table 11: External Roles

| Role | Description |
| --- | --- |
| SAP_BW_LPA_LP0 | Performs daily monitoring of point-of-sale activities for the purposes of investigating potential fraudulent activities.<br>For more information, see help.sap.com/bicontent > *<Your version of SAP NetWeaver BI Content>* > *Application Help* > *BI Content* > *Industry Solutions* > *Trading Industries* > *Retail Trade* > *Store Analytics* > *Loss Prevention Analytics* > *Roles* > *Loss Prevention Officer*.<br>• Cross-application Authorization Objects (AAAB): |

| Role | Description |
| --- | --- |
| | ○ Authorization Check for RFC Access<br>S_RFC field ACTVT has value: 16<br>S_RFC field RFC_NAME has values: RFC1, RRMX, RRXWS, RRY1, RSAH, RSBOLAP_BICS, RSBOLAP_BICS_CONSUMER, RSBOLAP_BICS_PROVIDER, RSBOLAP_BICS_PROVIDER_VAR, RSFEC, RSMENU RSOBJS_RFC_INTERFACE, RSOD_BIRM, RSRCI_LOCAL_VIEW, RSR_XLS_RFC, RSWAD, RSWRTEMPLATE, RS_BEX_REPORT_RFC, RS_IGS, RZX0, RZX2, SDIFRUNTIME, SM02, SMHB, SRFC, SUNI, SUSO, SYST, SYSU<br>S_RFC field RFC_TYPE has value: FUGR<br>○ Transaction Code Check at Transaction Start<br>S_TCODE field TCD has values:RRMX<br>• Basis: Administration (BC_A):<br>○ C calls in ABAP programs<br>S_C_FUNCT field ACTVT has value: 16 – Execute<br>S_C_FUNCT field CFUNCNAME has value: *<br>S_C_FUNCT field PROGRAM has value: *<br>• Basis - Central Functions (BC_Z):<br>○ Authorizations for Accessing Documents<br>S_BDS_D field ACTVT has value: *<br>S_BDS_D field LOIO_CLASS has value: *<br>○ Authorizations for Document Set<br>S_BDS_DS field ACTVT has value: *<br>S_BDS_DS field ACTVT has value: BW_*<br>S_BDS_DS field ACTVT has value: OT – Other Objects<br>○ Authorization Object for Sending<br>S_OC_SEND field COM_MODE has value: *<br>S_OC_SEND field NUMBER has value: *<br>• Business Information Warehouse (RS)<br>○ BI Authorizations in Role<br>S_RS_AUTH field BIAUTH has value: LOCATIO_AUTH<br>○ BEx Broadcasting Authorization to Schedule<br>S_RS_BCS field ACTVT has value: *<br>S_RS_BCS field RS_EVID has value: *<br>S_RS_BCS field RS_EVTYPE has value: *<br>S_RS_BCS field RS_OBJID has value: * |

| Role | Description |
| --- | --- |
| | S_RS_BCS field RS_OBJTYPE has value: *<br>○ Business Explorer - Components<br>S_RS_COMP field ACTVT has values: 01, 02, 03, 06, 16, 22<br>S_RS_COMP field RSINFOAREA has value: *<br>S_RS_COMP field RSINFOCUBE has value: *<br>S_RS_COMP field RSZCOMPID has value: *<br>S_RS_COMP field RZCOMPTP has values: CKF, REP, RKF, STR<br>○ Data Warehousing Workbench - InfoObject<br>S_RS_IOBJ field ACTVT has value: *<br>S_RS_IOBJ field RSIOBJ has value: *<br>S_RS_IOBJ field RSIOBJCAT has value: *<br>S_RS_IOBJ field RSIOBJPART has value: *<br>○ Data Warehousing Workbench - Aggregation Level<br>S_RS_ALVL field ACTVT has value: 03<br>S_RS_ALVL field RSALVLOBJ has value: *<br>S_RS_ALVL field RSINFOAREA has value: *<br>S_RS_ALVL field RSPLSALVL has value: *<br>○ Data Warehousing Workbench - MultiProvder<br>S_RS_MPRO field ACTVT has value: 03<br>S_RS_MPRO field RSMPROOBJ has value: *<br>S_RS_MPRO field RSINFOAREA has value: *<br>S_RS_MPRO field RSMPRO has value: *<br>○ Data Warehousing Workbench - InfoSet<br>S_RS_ISET field ACTVT has value: 03<br>S_RS_ISET field RSISETOBJ has value: *<br>S_RS_ISET field RSINFOAREA has value: *<br>S_RS_ISET field RSINFOSET has value: *<br>○ Business Explorer – Variants in Variable Screen<br>S_RS_PARAM field ACTVT has value: *<br>S_RS_PARAM field PARAMNM has value: * |

## OData Service Roles for SAP Customer Activity Repository

The table below shows the roles required to use the OData services provided with SAP Customer Activity Repository:

Table 12: OData Service Roles

| OData Service | Role |
| --- | --- |
| MaterialQueryResults | sap.is.retail.car.int.roles::MaterialQuery |

| OData Service | Role |
|---|---|
| MaterialInternationalArtINmbrQueryResults | sap.is.retail.car.int.roles::MaterialInternationalArtINmbrQuery |
| RetailLocationQueryResults | sap.is.retail.car.int.roles::RetailLocationQuery |
| POSSalesQueryResults | sap.is.retail.car.int.roles::POSSalesQuery |
| MultiChannelSalesQueryResults | sap.is.retail.car.int.roles::MultiChannelSalesQuery |
| InventoryVisibilityQueryResults | sap.is.retail.car.int.roles::InventoryVisibilityQuery |
| AnalyzeForecast.xsodata | sap.hba.t.rtl.udf.afc.roles::AnalyzeForecast |

## Standard Authorization Objects for SAP Customer Activity Repository

The table below shows the security-relevant authorization objects that are used by SAP Customer Activity Repository. For more information about an authorization object, call it up in transaction **SE80** and choose *Display Object Documentation*.

Table 13: Standard Authorization Objects

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| /POSDW/LPA | Authorization for Loss Prevention Analytics (LPA) | /POSDW/PTN | • ACTV: Active<br>• IACT: Inactive<br>• INIT: Initial<br>• NEW: New | Pattern Status |
| /POSDW/PTR | Authorization for POS Transaction Data | • /POSDW/STO<br>• /POSDW/PAC | • Selection from list of stores currently defined in customizing<br>• Values for /POSDW/PAC are:<br>  ○ 01 Add or Create<br>  ○ 03 Display<br>  ○ 06 Delete<br>  ○ 24 Archive<br>  ○ 31 Create TREX Index<br>  ○ 32 Index TREX<br>  ○ 34 Delete TREX Index | • Store<br>• Activities for Authorization for POS Transactions |
| W_POS_ADMI | Authorization for Administrative Tasks | • /POSDW/TAB<br>• /POSDW/ADC | 01 Assign tables to Placement Group Types | • Table Name<br>• Activities for Authorization for |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| | | | 02 Create Level 2 Range Partitions for TLOG tables<br>03 Delete Level 2 Range Partitions for TLOG tables<br>04 View Level 2 Range Partitions for TLOG tables | Administrative Tasks |
| W_POS_AGGP | Authorizations for initiating outbound processing in PIPE | • /POSDW/STO<br>• /POSDW/AGL<br>• /POSDW/OTS<br>• /POSDW/OAC | • Selection from list of stores currently defined in customizing<br>• Selection from list of aggregation levels currently defined in customizing<br>• Selection from list of outbound tasks currently defined in customizing<br>• Values for /POSDW/OAC are:<br>○ 16 Process Outbound Task<br>○ 85 Reverse Outbound Task | • Store<br>• Aggregation Level<br>• Task for Outbound Processing<br>• Activities for Outbound Processing in PIPE |
| W_POS_AGGR | Authorizations for performing aggregations in PIPE | • /POSDW/STO<br>• /POSDW/AGL<br>• /POSDW/AAC | • Selection from list of stores currently defined in customizing<br>• Selection from list of aggregation levels currently defined in customizing<br>• Values for /POSDW/AAC are:<br>○ 02 Create Aggregate | • Store<br>• Aggregation Level<br>• Task for Outbound Processing<br>• Activities for Aggregation in PIPE |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| | | | ○ 02 Change Aggregate<br>○ 03 Display Aggregate<br>○ 05 Close Aggregate<br>○ 06 Delete Aggregate<br>○ 24 Archive Aggregate<br>○ 25 Reload Aggregate | |
| W_POS_CCNR | Authorizations for credit card numbers in PIPE | • /POSDW/STO<br>• /POSDW/CAC | • Selection from list of stores currently defined in customizing<br>• Values for /POSDW/CAC are:<br>○ 02 Display Credit Card Number | • Store<br>• Activities for Authorization for Credit Card Numbers |
| W_POS_FSPR | Field Selection Profile | /POSDW/FSP | Selection from list of field selection profiles currently defined in customizing | |
| W_POS_STAT | Authorizations for PIPE-related tasks | • /POSDW/STO<br>• /POSDW/SAC<br>• /POSDW/TAS | • Selection from list of stores currently defined in customizing<br>• Values for /POSDW/SAC are:<br>○ 01 Process Task<br>• Selection from list of tasks currently defined in customizing | • Store<br>• Activities for Authorization for Task Status<br>• Task Code |
| W_POS_TIBQ | Authorizations for performing Inbound Queue operations in PIPE | • /POSDW/STO<br>• /POSDW/IAC<br>○ 01 Create<br>○ 02 Change<br>○ 03 Display | • Selection from list of stores currently defined in customizing | • Store<br>• Activities for TIBQ Authorization |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| | | ○ 06 Delete<br>○ 16 Process | • Values for /POSDW/IAC are: | |
| W_POS_TRAN | Authorizations for changing data in POS transactions | • /POSDW/STO<br>• /POSDW/PAC | • Selection from list of stores currently defined in customizing<br>• Values for /POSDW/PAC are:<br>○ 01 Add or Create<br>○ 03 Display<br>○ 06 Delete<br>○ 24 Archive<br>○ 31 Create TREX Index<br>○ 32 Index TREX<br>○ 34 Delete TREX Index | • Store<br>• Activities for Authorization for POS Transactions |
| W_POS_UNPR | Used to validate whether a store associate is authorized to view unprocessed transactions for a store | • /POSDW/PLT<br>• /POSDW/UAC | • 4-character customer-defined value<br>• 03 Display data | • Site number<br>• Activities permitted by the authorization |
| B_CCSEC | Unmasked display of credit card numbers | ACTVT | Values for ACTVT are:<br>• 03 Display<br>• 06 Delete<br>• 71 Analyze | |
| CA_POWL | Authorization for *Personal Object Worklist (POWL)* iViews for the POWL applications of Demand Data Foundation (DDF). | POWL_APPID<br>POWL_CAT<br>POWL_LSEL<br>POWL_QUERY<br>POWL_RA_AL<br>POWL_TABLE | | |
| S_START | Used when checking the start authorization for particular TADIR objects (such as Web Dynpro applications). | *Object Name*<br>*Object Type*<br>*Program ID* | /DMF/* and /PRM/*<br>POWL<br>WDYA<br>R3TR | |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| | **Do not** use this authorization object directly in your own coding. It can only be used through the `CL_START_AUTH_CHECK` class.<br>For more information about the start authorization check for program objects with object catalog entries, see SAP Note 1413011 . | | | |
| `/DMF/AOR` | Authorization for the *Maintain Area of Responsibility (AOR)* service on the SAP Easy Access screen. | `ACTVT` | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| `S_TCODE` | Transaction check at transaction start. | `TCD` | Report `/DMF/TS_DELETE`<br>`RSM37`<br>`SM37` | |
| `/DMF/CM_AT` | Authorization to assign attributes. | `ACTVT` | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| `/DMF/CM_IM` | Authorization to define images. | `ACTVT` | *02 Change*<br>*03 Display*<br>*06 Delete* | |
| `/DMF/DISCH` | Authorization for the distribution chain. | `ACTVT` | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| `/DMF/DMDTS` | Authorization to access demand time series data, including any business intelligence (BI) interfaces that would | `ACTVT` | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| | be sending point-of-sale (POS) data or generic consumption data. | | | |
| /DMF/EWB | Authorization for the exception handling framework. | ACTVT | *03 Display* | |
| /DMF/FCANA | Authorization to access forecasting and analytics. | ACTVT | *16 Execute*<br>*71 Analyze* | |
| /DMF/IMAGE | Authorization for the *Image* object. | ACTVT | *01 Create or generate* | |
| /DMF/INV | Authorization for the *Inventory* object. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/LANE | Authorization for the *Transportation Lane* object. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/LBUI | Authorization for the load balancing configuration and user interface for the DDF server configuration. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete*<br>*32 Save* | |
| /DMF/LOC | Authorization for the *Location* object. | ACTVT | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/LOCHR | Authorization for the *Location Hierarchy* object. | ACTVT | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/ME | Authorization for the *Monitor Exceptions* service on the SAP Easy Access screen. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| /DMF/MI | Authorization check for the *Monitor Imports* service on the SAP Easy Access screen. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/OFRSO | Internal organizational unit identifier for the distribution channel. | /DMF/CHCHK (first input value for this authorization object) | All activities | |
| /DMF/OFRSO | Internal organizational unit identifier for the sales organization. | /DMF/SOCHK (second input value for this authorization object) | All activities | |
| /DMF/OPUI | Authorization to access the user interface of the *Schedule Model and Forecasts* service on the SAP Easy Access screen. | ACTVT | *03 Display*<br>*16 Execute* | |
| /DMF/PHP | Authorization for the *Placeholder Product* object. | ACTVT | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/PROD | Authorization for the *Product* object. | ACTVT | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete*<br>*61 Export* | |
| /DMF/PRDHR | Authorization for the *Product Hierarchy* object. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/PRDLC | Authorization for the *Product Location* object in the consumer access layer. | ACTVT | *01 Create*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |

| Authorization Object | Authorization Object Description | Field | Value | Field Description |
|---|---|---|---|---|
| /DMF/TS | Authorization for the *Time Series Data* object in the access layer. | ACTVT | *01 Create or generate*<br>*02 Change*<br>*03 Display*<br>*06 Delete* | |
| /DMF/SLSH | Authorization for the *Sales History* object. | ACTVT | *01 Create*<br>*03 Display*<br>*06 Delete* | |

### Standard Authorization Objects for On-Shelf Availability

The table below shows the security-relevant authorization objects that are used by the On-Shelf Availability (OSA) module in SAP Customer Activity Repository.

Table 14: Standard Authorization Objects

| Authorization Object | Field | Value | Description |
|---|---|---|---|
| /OSA/DEPT | /OSA/AREA<br>/OSA/STORE<br>ACTVT | EMPLOYEE,<br>MANAGER<br>03 | Display authorization for the department |
| /OSA/PROD | /OSA/AREA<br>/OSA/STORE<br>ACTVT | EMPLOYEE,<br>MANAGER<br>02, 03 | Change and display authorization for the product |
| /OSA/STOR | /OSA/STORE<br>ACTVT | <br>03 | Display authorization of the store |
| /OSA/ADM | /OSA/ADM_A | 02, 05 | Execute On-Shelf Availability Dispatcher<br>Archive On-Shelf Availability Status Log |

All exposed APIs to retrieve the store, department, and product information have an integrated verification to ensure that the calling user has the necessary authorizations to perform the action. If the user does not have the necessary permissions, an error is returned to the caller and no data/information is provided. If you want to restrict access, you can do so by changing the values of the relevant authorization objects.

## 6.1 Authorization Requirements for the UDF AFL

In this procedure you set up the privileges required for the Unified Demand Forecast application function library (UDF AFL).

> **Note**
>
> This procedure is part of the *Activate SAP HANA Content for SAP Customer Activity Repository* procedure, as described in the *Common Installation Guide*. See help.sap.com/car > *<your release>* > *Installation and*

## Overview

To set up the required privileges, you first create the following roles in SAP HANA studio, then grant each role specific privileges, and finally assign the roles to specific users:

Table 15

| Roles for the UDF AFL | Description |
|---|---|
| `UDF_EXECUTE` | Defines all privileges for executing UDF; enables the `SAP<SID>` user to execute UDF. |
| `UDF_DEPLOY` | Defines all privileges for deploying the SAP HANA content for UDF; required to import and activate the SAP HANA content. |
| `UDF_DEPLOY_SYS_REPO` | Defines additional privileges for the `_SYS_REPO` standard user; required to activate the SAP HANA content. |

Additionally, we have provided example SQL statements that you can use and adapt as needed.

If you are familiar with roles and privileges in SAP HANA studio, you can skip directly to the *Prerequisites* section below. If you want more background first, continue with the next section.

## Background

### Authorization Concept

The UDF AFL relies on the access control mechanisms of the SAP HANA database. SAP HANA has implemented the regular SQL authorization concept based on privileges. The privileges provide access to views and procedures in the SAP HANA content, which in turn provide access to data and functionality directly on the database level.

You can grant privileges to a user either directly or indirectly (through roles). We recommend that you grant privileges through roles. A role is a collection of privileges. You can grant roles to users and to other roles.

For more information, see the following sections under help.sap.com/hana_platform > *Security* > *SAP HANA Security Guide*:

- *SAP HANA User Management*
- *SAP HANA Authentication and Single Sign-On*
- *SAP HANA Authorization* (privilege types and roles)

### Managing Users, Roles, Privileges, and Schemas in SAP HANA Studio

Here is some general information to help you with the procedure below:

- You can find the *Users* and *Roles* in the *Security* folder of your back-end system in SAP HANA studio.
- When you select a role, a details screen opens where you can grant and remove privileges and other roles.
- When you create a database user (such as `SAP<SID>`), a database schema of the same name is created automatically.
- You can find the schemas in the *Catalog* folder.
- SQLScript procedures are always assigned to a specific schema. For example:
  - Schema `_SYS_BIC` includes the modeling and forecasting procedures used by the UDF AFL.
  - Schema `_SYS_AFL` includes the actual UDF AFL procedures.
- Some technical users are available as standard, for example `_SYS_REPO`.

### Prerequisites

- You have installed the UDF AFL in your SAP HANA database as described in ▶ help.sap.com/car ↗ ▶ *<your release>* ▶ *Installation and Upgrade Information* ▶ *Installation Guide* ▶ *Implementation Scenarios* ▶ *SAP Customer Activity Repository* ▶ *Installation* ▶ *Install ABAP Back-End Server* ▶ *Install SAP Customer Activity Repository Retail Applications Bundle* ◀.
- You have an `SAP<SID>` user and schema in your SAP HANA database (the names must be identical).
- You have checked that the correct schemas are mapped for your back-end system in SAP HANA studio. The setting under ▶ *SAP HANA Modeler* ▶ *Schema Mapping* ◀ must be as follows:

  Table 16

| Authoring Schema | Physical Schema |
|---|---|
| `SAP_DDF` | `SAP<SID>` |

- You have done steps 1 to 3 of the *Activate SAP HANA Content for SAP Customer Activity Repository* procedure.

### Procedure

In this procedure, you create the three roles for the UDF AFL, grant the required privileges, and assign the roles to specific users:

1. Select your back-end system in SAP HANA studio and open the *SAP HANA Administration Console*.
2. Navigate to ▶ *Security* ▶ *Roles* ◀, right-click, and select *New Role*.
3. Enter **`UDF_EXECUTE`** as the role name.

   SQL example: **`create role UDF_EXECUTE;`**
4. Make the following settings for this role:
   - *Granted Roles*: `AFL__SYS_AFL_UDFCORE_AREA_EXECUTE`

     SQL example: **`grant AFL__SYS_AFL_UDFCORE_AREA_EXECUTE to UDF_EXECUTE;`**
   - *Object Privileges*:
     - For catalog object (schema) `SAP<SID>`: *SELECT*, *INSERT*, *UPDATE*, *DELETE*

       SQL example: **`grant SELECT, INSERT, UPDATE, DELETE on schema SAP<SID> to UDF_EXECUTE;`**
     - For catalog object (schema) `_SYS_BIC`: *SELECT*, *EXECUTE*

       SQL example: **`grant SELECT, EXECUTE on schema _SYS_BIC to UDF_EXECUTE;`**
   - *Analytic Privileges*: `_SYS_BI_CP_ALL`

     SQL example: **`call GRANT_ACTIVATED_ANALYTICAL_PRIVILEGE('_SYS_BI_CP_ALL','UDF_EXECUTE');`**

   Save your settings. You have successfully set up the first role.
5. Open the details screen for user `SAP<SID>` and assign the role:
   - *Granted Roles*: `UDF_EXECUTE`

     SQL example: **`grant UDF_EXECUTE to SAP<SID>`**

   Save your settings.
6. Navigate again to ▶ *Security* ▶ *Roles* ◀, right-click, and select *New Role*.
7. Enter **`UDF_DEPLOY`** as the role name.

   SQL example: **`create role UDF_DEPLOY;`**

8. Make the following settings for this role:
   - *Granted Roles*: `CONTENT_ADMIN`

     SQL example: **`grant CONTENT_ADMIN to UDF_DEPLOY;`**
   - *System Privileges*: `CATALOG READ`

     SQL example: **`grant CATALOG READ to UDF DEPLOY;`**

   Save your settings.
9. Open the details screen for user `SAP<SID>` and assign the role:
   - *Granted Roles*: `UDF_DEPLOY`

     SQL example: **`grant UDF_DEPLOY to SAP<SID>`**

   Save your settings. You have successfully set up the second role.
10. Navigate again to *Security* > *Roles*, right-click, and select *New Role*.
11. Enter **`UDF_DEPLOY_SYS_REPO`** as the role name.

    SQL example: **`create role UDF_DEPLOY_SYS_REPO;`**
12. Make the following settings for this role:
    - *Object Privileges*:
      - For catalog object (schema) `SAP<SID>`: *SELECT*, *INSERT*, *UPDATE*, *DELETE*

        SQL example: **`grant SELECT, INSERT, UPDATE, DELETE on schema SAP<SID> to UDF_DEPLOY_SYS_REPO;`**

    Save your settings. You have successfully set up the third role.
13. Open the details screen for user `_SYS_REPO` and assign the role:
    - *Granted Roles*: `UDF_DEPLOY_SYS_REPO`

      SQL example: **`grant UDF_DEPLOY_SYS_REPO to _SYS_REPO;`**

    Save your settings.

### Result

You have successfully set up the roles and privileges for the UDF AFL. You can now continue with the next steps of the *Activate SAP HANA Content for SAP Customer Activity Repository* procedure.

# 7 Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management.

We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

### Session Security Protection on the AS ABAP

To activate session security on the AS ABAP, set the corresponding profile parameters and activate the session security for the client(s) using the transaction SICF_SESSIONS.

For more information, a list of the relevant profile parameters, and detailed instructions, see *Activating HTTP Security Session Management on AS ABAP* in the AS ABAP security documentation.

# 8 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for the SAP Customer Activity Repository application is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to the SAP Customer Activity Repository. Details that specifically apply to the SAP Customer Activity Repository application are described in the following topics:

- Communication Channel Security

  This topic describes the communication paths and protocols used by the application.
- Network Security

  This topic describes the recommended network topology for the application. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate the application.
- Communication Destinations

  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the *SAP NetWeaver Security Guide*:

- *Network and Communication Security*
- *Security Guides for Connectivity and Interoperability Technologies*

## 8.1 Communication Channel Security

The table below shows the communication paths used by SAP Customer Activity Repository, the protocol used for the connection, and the type of data transferred.

Table 17: Communication Paths

| Communication Path | Protocol Used | Type of Data Transferred | Data Requiring Special Protection |
|---|---|---|---|
| Front-end client using SAP GUI for Windows to application server | DIAG | All application data | Passwords, credit card information |
| Application server to third-party application | HTTPS | System ID, client, and host name | System information (host name), personal data, |

| Communication Path | Protocol Used | Type of Data Transferred | Data Requiring Special Protection |
|---|---|---|---|
| | | | transactional data, and credit card information |
| Document upload | HTTPS | XML document | Personal data, transactional data, and credit card information |
| Application server to application server | RFC | Application data | System information, personal data, transactional data, and credit card information |
| Application server to application server | IDoc | Application data records | Personal data, transactional data, and credit card information |
| Web service client to Web service provider | SOAP | XML document | Personal data, transactional data, and credit card information |

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

For more information, see *Transport Layer Security* the *SAP NetWeaver Security Guide*.

> **Recommendation**
>
> We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see *Transport Layer Security* and *Web Services Security* in the *SAP NetWeaver Security Guide*.

## 8.2 Network Security

The network topology for SAP Customer Activity Repository is based on the topology used by the SAP NetWeaver platform. Therefore, refer to the following documentation for information on network security:

- SAP NetWeaver 7.40 Security Guide
- SAP Supply Chain Management Security Guide
- SAP Supplier Relationship Management Security Guide
- SAP ERP Central Component Security Guide
- SAP Customer Relationship Management Security Guide

If you are implementing the Loss Prevention Analytics functionality, you should also refer to the following documentation:

- Security Guide for SAP NetWeaver BW
- Portal Security Guide

To locate the security guides listed above, go to SAP Help Portal (help.sap.com), choose your product and then choose Security Information. For example, help.sap.com/nw74 > *Security Information* > *Security Guide*.

### Ports

SAP Customer Activity Repository runs on SAP NetWeaver and uses the ports from the AS ABAP. For more information, see the topics for *AS ABAP Ports* in the corresponding *SAP NetWeaver Application Server ABAP Security Guide* . For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, see also the document *TCP/IP Ports Used by SAP Applications*, which is located on SAP Community Network (SCN) at scn.sap.com/community/security under *Infrastructure Security* > *Network and Communication Security*.

## 8.3 Communication Destinations

The incorrect configuration of users and authorizations for connection destinations can result in high security flaws. To ensure the proper configuration of users and authorizations, do the following:

- Choose the appropriate user type: Communication or System
- Assign only the minimum required authorizations to a user type
- Choose a secure and secret password for a user type
- Store only connection user logon data for System user types
- Choose trusted system functionality

Connection destinations are particularly important in SAP Customer Activity Repository for connecting incoming datasources and outgoing destinations. SAP Customer Activity Repository does not provide any pre-configured RFC destinations; these destinations are created by customers. Therefore, connection information (such as connection type, user name and password) is not defined directly within SAP Customer Activity Repository; it relies on references to system-defined and/or system-administered connections, for example, RFC destinations or Web service configurations.

You require RFC destinations to connect SAP and non-SAP systems to SAP Customer Activity Repository. If communication is to be accomplished with IDocs using Application Link Enabling (ALE), you may require additional ALE configurations to ensure that the applicable message types are correctly routed.

For inbound communication to SAP Customer Activity Repository, you must do the following:

- Define SAP Customer Activity Repository as a target destination within the source system, for example, as an RFC destination with a specific user identified.
- Define a user with the necessary authorizations for SAP Customer Activity Repository

For outbound communication from SAP Customer Activity Repository, you must do the following:

- Define all target destinations within SAP Customer Activity Repository, for example, as an RFC destination with a specific user identified for the target system.
- Configure SAP Customer Activity Repository Customizing as the target destinations.
- Define all users with the necessary authorizations on the target system(s).

The table below shows an overview of the communication destinations used by the SAP Customer Activity Repository application.

Table 18: Connection Destinations

| Destination | Delivered | Type | User, Authorizations | Description |
|---|---|---|---|---|
| Customer-defined in external system | No | RFC | • S_ICF (for client system)<br>• S_RFC (for server system)<br>• S_RFCACL (for trusted systems only)<br>• W_POS_TIBQ (Activity '01' Create) | Inbound transaction data from BAPI call |
| Customer-defined through communication channel (either at runtime or configured for proxy/logical port) in external system | No | HTTP(S) | Web Service Authorization Objects:<br>• S_SERVICE<br>Web Service Roles:<br>• SAP_BC_WEBSERVICE_CONSUMER | Inbound transaction data from Web Service call (from POS) |
| Customer-defined in external system | No | tRFC | • S_ICF (for client system)<br>• S_RFC (for server system)<br>• S_RFCACL (for trusted systems only)<br>• W_POS_TIBQ (Activity '01' Create) | Inbound transaction data from IDOC through ALE (such as for SAP Retail, etc.) |
| Customer-defined in Customizing | No | RFC | RFC Authorization Objects:<br>• S_ICF (for client system)<br>• S_RFC (for server system)<br>• S_RFCACL (for trusted systems only)<br>ALE Authorization Objects:<br>• B_ALE_RECV<br>• B_ALE_REDU<br>Authorization Objects: | Outbound transaction data from BAPI / Function Module resulting from Task Processing (such as for SAP ERP, SAP F&R, Credit Card Settlement, Payment Card, , etc.) |

| Destination | Delivered | Type | User, Authorizations | Description |
|---|---|---|---|---|
| | | | • W_POS_AGGP<br>Roles:<br>• /POSDW/ ADMINISTRATOR<br>• /POSDW/ SALES_AUDIT | |
| Customer-defined through communication channel (either at runtime or configured for proxy/logical port) of SAP Customer Activity Repository system | No | HTTP(S) | Web Service Authorization Objects:<br>• S_SERVICE<br>Web Service Roles:<br>• SAP_BC_WEBSERVICE_CONSUMER<br>Authorization Objects:<br>• W_POS_AGGP<br>Roles:<br>• /POSDW/ ADMINISTRATOR<br>• /POSDW/ SALES_AUDIT | Outbound transaction data from Web Service call resulting from Task Processing (such as for SAP CRM) |
| Customer-defined in external system | No | tRFC | RFC Authorization Objects:<br>• S_ICF (for client system)<br>• S_RFC (for server system)<br>• S_RFCACL (for trusted systems only)<br>Authorization Objects:<br>• W_POS_TIBQ (Activity '01' Create) | Outbound transaction data from IDOC resulting from Task Processing (such as for SAP Retail, etc.) |

# 9 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For the SAP Customer Activity Repository application (and specifically for POS Data Management component), the following service is required:

Table 19

| Service | Description |
|---|---|
| POSTRANSACTERPBLKCRTRQ | Inbound POS Transactions Service |

For Loss Prevention Analytics (LPA) services within the SAP NetWeaver Portal, the following services are required:

Table 20

| Service | Description |
|---|---|
| LPA_WDA_CASHIERLOOKUP | Cashier Lookup |
| LPA_WDA_TXN_VIEWER | Transaction Viewer |
| LPA_WDA_JOURNAL_VIEWER | Journal Viewer |
| You only need to activate these services if you are using LPA functionality. For more information, see SAP Note 1533599. | |

You activate these services using transaction SICF. If your firewall(s) use URL filtering, note the URLs used for the services and adjust your firewall settings accordingly.

For information about activating and deactivating ICF services, see *Activating and Deactivating ICF Services* in the *SAP NetWeaver Library* documentation.

For information about ICF security, see the *RFC/ICF Security Guide* within the *Security Guides for Connectivity and Interoperability Technologies* in the *SAP NetWeaver Security Guide*.

# 10 Data Storage Security

## Data Storage

The SAP Customer Activity Repository application saves data in the SAP HANA database of the SAP system (configuration, master, transactional, and aggregation data). Data access for users is controlled through the standard SAP NetWeaver and SAP HANA authorization concepts (see the *Authorizations* [external document] section).

The application makes use of data originating from other SAP systems (for example, SAP ERP, and optionally SAP CRM). SAP Customer Activity Repository accesses data using SAP HANA read-only views included in SAP HANA Live for SAP ERP and SAP HANA Content for SAP Customer Activity Repository. The data is protected through the implementation of the SAP HANA Live for Business Suite authorization concept, which relies on SAP HANA DB object and analytical privileges for users.

Data is not temporarily stored in the file system for any reason. For non-temporary data storage, see the subsequent section for information about file system storage for archived transactional and aggregation data.

### Using Logical Path and File Names to Protect Access to the File System

The SAP Customer Activity Repository application can optionally save data in files in the file system (specifically for archiving purposes). Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory (including subdirectories) that does not match a stored mapping, then an error occurs.

The following lists show the logical file names and paths used by the SAP Customer Activity Repository application and for which programs these file names and paths apply:

**Logical File Names Used in This Application**

The following logical file names have been created in order to enable the validation of physical file names:

- `ARCHIVE_DATA_FILE_POSDW`
  - Programs using this logical file name and parameters used in this context:
    - Archiving object `/POSDW/TL`
    - Program `/POSDW/ARCHIVE_READ`
    - Program `/POSDW/ARCHIVE_WRITE`
    - Program `/POSDW/ARCHIVE_DELETE`
    - Program `/POSDW/ARCHIVE_RELOAD`
  - Parameters used in this context ('_' between parameters, and suffix of '`_TL.ARCHIVE`'):
    - `<PARAM_1>`
    - `<PARAM_3>`
    - `<DATE>`
    - `<TIME>`
    - `<PARAM_2>`
- `ARCHIVE_DATA_FILE_POSDW2`

    - Programs using this logical file name:
        - Archiving object `/POSDW/AGG`
        - Program `/POSDW/ARCHIVE_READ_AGGERGATE`
        - Program `/POSDW/ARCHIVE_WRITE_AGGREGATE`
        - Program `/POSDW/ARCHIVE_DELE_AGGREGATE`
    - Parameters used in this context ('_' between parameters, and suffix of '`_AG.ARCHIVE`'):
    - `<PARAM_1>`
    - `<PARAM_3>`
    - `<DATE>`
    - `<TIME>`
    - `<PARAM_2>`
- `ARCHIVE_DATA_FILE_POSDW_F`
    - Programs using this logical file name:
        - Archiving object `/POSDW/TLF`
        - Program `/POSDW/ARCHIVE_READ_HDB_F`
        - Program `/POSDW/ARCHIVE_WRITE_HDB_F`
        - Program `/POSDW/ARCHIVE_DELETE_HDB_F`
        - Program `/POSDW/ARCHIVE_RELOAD_HDB_F`
    - Parameters used in this context ('_' between parameters, and suffix of '`.ARCHIVE`'):
        - `<PARAM_1>`
        - `<PARAM_3>`
        - `<DATE>`
        - `<TIME>`
        - `<PARAM_2>`

#### Logical Path Names Used in This Application

The logical file names listed above all use the logical file path `ARCHIVE_GLOBAL_PATH`.

#### Activating the Validation of Logical Path and File Names

These logical paths and file names, as well as any subdirectories, are specified in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions `FILE` (client-independent) and `SF01` (client-specific). To find out which paths are being used by your system, you can activate the corresponding settings in the Security Audit Log.

For more information, see:

- *Logical File Names* in the *SAP NetWeaver Library*
- *Protecting Access to the File System* in the *SAP NetWeaver Application Server ABAP Security Guide*
- *Security Audit Log* in the *SAP NetWeaver Library*

## Data Protection

The SAP Customer Activity Repository application does not support or require a Web Browser as its user interface, and therefore does not use cookies to store data on the front-end. Additionally, no data is stored on a client.

The application transactional data may contain sensitive data, in the form of credit card numbers, and so on, which are provided from outside systems. It is strongly recommended that all such data be encrypted at its source, remain encrypted when passed between systems, and remain encrypted within the SAP Customer Activity Repository's application database tables or file system. For specific steps necessary to support or provide for data encryption, see the relevant SAP Notes in section Before You Start [page 9].

For business use-cases where the decryption of this type of data is required, specific authorizations are necessary and access is logged for auditing purposes. For more information, see the *Authorizations* [external document] section.

# 11 Security for Additional Applications

The SAP Customer Activity Repository application does not have any additional third-party applications associated with it or delivered with it, nor does it have any mandatory dependencies on third-party applications.

For customer scenarios when third-party applications are optionally used, the relevant security settings for the applicable application should be considered in combination with those of the SAP Customer Activity Repository application.

Please refer to the Fundamental Security Guides information in the Before You Start [page 9] section for additional security topics relating to the use of other SAP systems (SAP ERP, SAP CRM, and so on) within the overall solution.

The SAP HANA Live for SAP ERP is a pre-requisite for SAP Customer Activity Repository, and additionally the associated Analytics Authorization Assistant 1.0 tool used within the HANA Developer Studio tool is likewise required for the execution of the SAP Customer Activity Repository authorization concept. The only relevant security settings for the use of this tool are that the system administrator has granted the necessary privileges to the specific database user responsible for administering analytical privileges (please refer to the Analytics Authorization Assistant documentation for further details).

# 12 Enterprise Services Security

The following sections in the *SAP NetWeaver Security Guide* and documentation are relevant for all enterprise services delivered with the POS Data Management component of SAP Customer Activity Repository:

- *Web Services Security*
- *Recommended WS Security Scenarios*
- *SAP NetWeaver Process Integration Security Guide*

# 13 Payment Card Security According to PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was developed jointly by major credit card companies to create a set of common industry security requirements for the protection of credit card holder data. Compliance with this standard is relevant for companies processing credit card data. For more information, see www.pcisecuritystandards.org.

This section is provided to assist you in implementing payment card security aspects. It also presents issues that you must consider in order for your deployment to be PCI-DSS compliant.

> **Caution**
>
> PCI-DSS includes more than the issues and information provided in this section. Ensuring that your system is PCI-DSS compliant is entirely the customer's responsibility. SAP is not responsible for ensuring that a customer is PCI-DSS compliant.

The PCI-DSS compliance information provided in this guide is application-specific. For general information on ensuring payment card security, see: help.sap.com/ *SAP Business Suite* > *SAP ERP* > *SAP ERP Central Component* > *Security Information* > *SAP Service Marketplace* > *EHP 5* > *SAP ERP Security Guides* > *Payment Card Security*.

For updated general PCI-DSS information, see also SAP Note 1609917.

## 13.1 Credit Card Usage Overview

The SAP Customer Activity Repository is an integral part of the Store Connectivity scenario. It is possible that each connection contains PCI-relevant data. As such, each communication line displayed in the diagram below could be subject to the PCI-DSS, as could each component. (PCI-DSS implications for each component are discussed in the individual security guides).

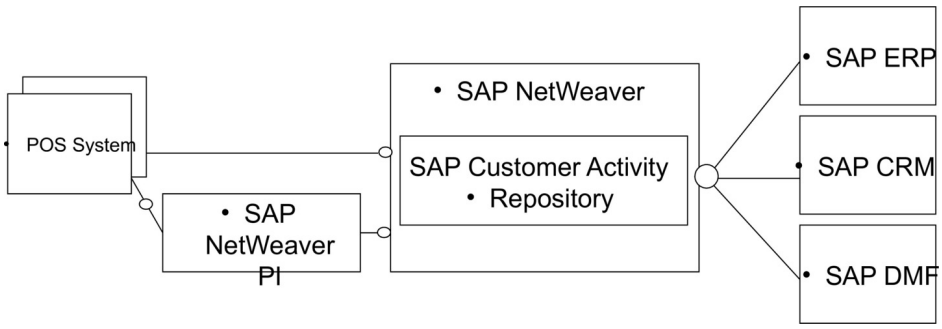



Figure 3: Communication Lines

## 13.1.1 SAP Customer Activity Repository

### SAP Customer Activity Repository

SAP Customer Activity Repository can be used to support the Sales Audit transaction, during which credit card settlements are reviewed. As such, it must be configured to allow the Sales Auditor to access credit card data. SAP Customer Activity Repository can also serve as a transaction repository, where transactional data (including credit card data) can be aggregated and forwarded to other systems (Credit Card Settlement, SAP CRM, and SAP NetWeaver BW [for BI Content]) for additional processing.

SAP Customer Activity Repository's PIPE (included in the POS Data Management component) includes the following functionality to support your PCI-DSS compliance:

- Encryption of credit card data within PIPE using the `SAPCRYPTOLIB` encryption library
- Decryption of credit card data and decrypted display within PIPE
- Tracing and logging of decryption requests within PIPE
- Masking the display of credit card data in the POS Workbench
- Managing and distributing keys to the source POS

## 13.1.2 Detailed Data Flow of Credit Card Data

The PCI-DSS relevant data within a POS transaction consists of credit card data that can be stored within an application, and sensitive authentication data that must not be stored within an application.

Credit card data is transferred as part of the POS transaction data from a POS to SAP Customer Activity Repository; the service code is not transmitted with this data. Depending on the configuration of your transaction transfer application, the credit card data can be unencrypted or encrypted (symmetrically in an asymmetric envelope) using the PAYCRV application.

You can configure your system to transfer the credit card data using the HTTPS communication protocol, regardless of how the individual parts of the TLOG are encrypted.

The data is transferred from the POS to SAP Customer Activity Repository as follows:

1. The SOAP adapter residing in the adapter engine, the J2EE Stack, processes the HTTPS request. The SOAP adapter calls additional EJBs to encrypt the message, but the payload itself does not use SOAP-enveloping. Optionally, encrypted parts of the payload can be decrypted.
2. The SOAP adapter replaces all credit card data with dummy values and appends a privacy container as an RSA-encrypted attachment to the XML message using the SAP Store, Secure and Forward (SSF) API.
3. The XML messages are mapped to the format of the SAP Customer Activity Repository inbound interface and forwarded to SAP Customer Activity Repository through an RFC adapter (which also resides in the adapter engine).

   You can configure the communication to use Secure Network Communication (SNC) for the Remote Function Call (RFC), which results in an encrypted data transfer between the SAP NetWeaver PI and SAP Customer Activity Repository.

   During the lifetime of a message in SAP NetWeaver PI, all credit card data is stored in the database as part of the encrypted XML message attachment (both on the ABAP stack and the J2EE stack).
4. SAP Customer Activity Repository receives the TLOG messages and stores the content within the TLOG table in the transactional database.

5. The credit card data is separated as follows:
    - The credit card holder's name and the card's expiration date are stored in unencrypted format in the TLOG table. (The TLOG table content can be accessed by an authorized user in the POS Workbench, where the data is displayed in clear text format.)
    - The Permanent Account Number (PAN) is stored in encrypted and secure format using the PAYCRV application.

Only users with the required authorization can view the PAN in clear text format. Authorized users can request that the PAN be displayed in clear text format by choosing the corresponding button in the interface. Each time a user requests to view a PAN unmasked, it is logged in the application log.

1. The IDoc containing the POS transactional data is sent from SAP Customer Activity Repository to the SAP ERP POS Inbound over HTTPS. During the process, all PCI-DSS relevant data is unencrypted.
2. SAP ERP POS Inbound stores the data with an unencrypted or encrypted PAN using the PAYCRV application.

## 13.2 PCI-Related Customizing

### 13.2.1 SAP Basis Customizing Prerequisites

SAP Customer Activity Repository PCI-DSS Security Customizing settings enhance the Customizing settings of SAP Basis. The required SAP Basis Customizing settings consist of:

- Installing and configuring the `SAPCRYPTOLIB` encryption library
- Establishing the payment card security settings
- Configuring the key versioning

Depending on your system, you may require additional configurations. Check your system to verify if you need to set up any of the following:

- Your POS to use the public key and version for encryption
- Your POS to transfer secured credit card data with the public key
- SAP NetWeaver PI for secure handling of the credit card data
- SAP ERP, SAP CRM, or other subsequent systems for secure handling of credit card data
- Secure IDoc and BAdI communication

#### 13.2.1.1 Installation of the Encryption Library SAPCRYPTOLIB

The `SAPCRYPTOLIB` encryption library contains the functions required to encrypt credit card numbers.

You can define general settings for the execution of the encryption software in Customizing under *SAP NetWeaver* > *Application Server* > *System Administration* > *Maintain the Public Key Information for the System*.

For more information on installing the `SAPCRYPTOLIB` encryption library, see the section *Installing SapCryptolib* in SAP Note 662340.

If you set the encryption with the `SSFA` transaction, you must use the `PAYCRV` application.

## 13.2.1.2 Payment Card Security Settings

Payment card security settings are applied to all newly created or changed POS transactions that include credit card information.

### Basic Settings

You must configure the checking rules for payment card types as described in Customizing under *Cross-Application Components* > *Payment Cards* > *Basic Settings* > *Assign Checking Rule*. These rules are used for entering the payment card number. To avoid possible errors when making entries, you can use the checking rules to verify that you have met the conditions of the relevant payment card type.

### Settings for Payment Card Security

You must configure settings for the encryption, masking and access logs of payment cards. For information on configuring the settings, see Customizing under *Cross-Application Components* > *Payment Cards* > *Basic Settings* > *Make Security Settings for Payment Cards*.

> **Note**
>
> For SAP NetWeaver 7.0, you can access this activity from *Maintain View* `V_TCCSEC`.

Sample settings are as follows:

- *Security Level* – *Masked Display and Encrypted When Saved*
- *Access Log* – *Logging of Unmasked Display*
- *Additional Authorization Check for Unmasked Display* – Enabled
- Visible Characters for Masking:
  - *At Start* – 4
  - *At End* – 4
  - *Key Replacement Active* – Enabled

> **Note**
>
> To enable encryption, choose the *Masked Display and Encrypted When Saved* option in the *Security Level* field.

> **Caution**
>
> If you select the *Masked Display, Not Encrypted When Saved* as the security level, credit card numbers may be lost in the SAP system. Only choose this setting if the payment data is not to be processed any further.

### Maintain Payment Card Types

You must execute the steps described in this section only if you have set the *Masked Display and Encrypted When Saved* security level to the values described in the previous section.

To specify if payment card numbers for a credit card institution must be encrypted, enter the payment card type and assign a check rule. If you want to enable data encryption for a credit card type, choose the encryption check box.

For detailed instructions, see Customizing under *Cross Application Component* > *Payment Cards* > *Maintain Payment Card Type*.

> **Caution**
> Note that if the encryption indicator for a credit card institution is not set, but the general security level is set to *Masked Display and Encrypted Save*, the security level for the credit card institution will be lowered to *Masked Display, No Encrypted Save*.

### Masking Credit Card Number in IDocs

The `WECRYPTDISPLAY` transaction allows you to mask the display of credit card numbers in IDocs. To do so, you must make the following entries in the *Assignment: Encrypted Segment Field Display* table:

- *Message Type*: **`WPUBON`**
- *Segment Type*: **`E1WPB06`**
- *Field Name*: **`KARTENNR`**

### ERP Customizing - Customizing of Encryption Save Mode

The Customizing of Encryption Save Mode allows you to specify if existing Globally Unique Identifiers (GUIDs) can be reused for different credit cards. You can create your own BAdI implementation. If you do not create your own, the application uses the following existing GUID:

Enhancement spot: `ES_WPOS_PCA_SECURITY`

BAdI definition: `WPOS_PCA_SECURITY`

## 13.2.2 SAP Customer Activity Repository Customizing

### SAP Customer Activity Repository Customizing

In addition to the configuration settings described in the *SAP Basis Customizing Prerequisites* section, the SAP Customer Activity Repository Customizing activity defines how to store, process, and use sensitive data. For more information, see *SAP Customer Activity Repository* > *POS Data Management* > *POS Inbound Processing* > *General Settings* > *Define Security Profiles*.

The table below shows the settings for the encrypted storage of payment card numbers and how they are displayed on the User Interface. The encryption and display settings are:

Table 21

| Setting | Description | Example |
|---|---|---|
| Security Profile | Displays the identifier of the security profile. | 0001 |
| Description | Describes the security profile. | SAP Standard Security Profile |
| SSF Application | Identifies the `STRUST` application, which is part of SAP Basis. | `PAYCRV` (versioned keys) |
| Save Mode | Indicates whether the reference of the encrypted payment card number, which is a GUID (Globally Unique Identifier), is always re-used for the same payment card number. Otherwise different | Reuse Existing Entry |

| Setting | Description | Example |
| --- | --- | --- |
| | GUIDs are assigned for the same payment card number.<br>There is a trade-off between performance and increasing encryption table size during encryption, but there is no performance impact during decryption.<br>As an example, this could provide you with the option to Re-use Existing Entry for a cross-selling analysis of a credit card number or GUID in a further process/system. This setting does not affect your PCI-DSS compliancy. However, according to PCI-DSS, cross-selling analysis with card numbers should not be used, and data mining on a credit card could invalidate your PCI-DSS compliancy. | |
| Security Check | The security check must be set to *Allow Security Level Check* to be compliant with the PCI-DSS standard. This allows SAP Customer Activity Repository to work and check according to the payment card settings in the `TCCSEC` table in SAP Basis. | Allow Security Level Check |

## 13.3 Rotation or Changing of Encryption Keys

To be PCI-DSS compliant, encryption keys must be changed on a regular basis. See SAP Note 1151936 for more information about key replacement for encryption of payment card data.

### 13.3.1 Key Distribution Web Service

PCI-DSS requires that credit card data must be encrypted if it is transmitted over open, public networks. To fulfill this requirement, the Key Distribution Web service was implemented for the distribution of X.509 certificates. The Web service was under the NetWeaver governance approach. No SAP Business Objects or ARIS content are delivered with the Web service.

## 13.3.2 Pull Mechanism in SAP Customer Activity Repository

A pull mechanism is used between SAP Customer Activity Repository and the POS. The POS is the Web service consumer and SAP Customer Activity Repository is the service provider. The communication between the two systems is peer-to-peer and does not use SAP NetWeaver PI.

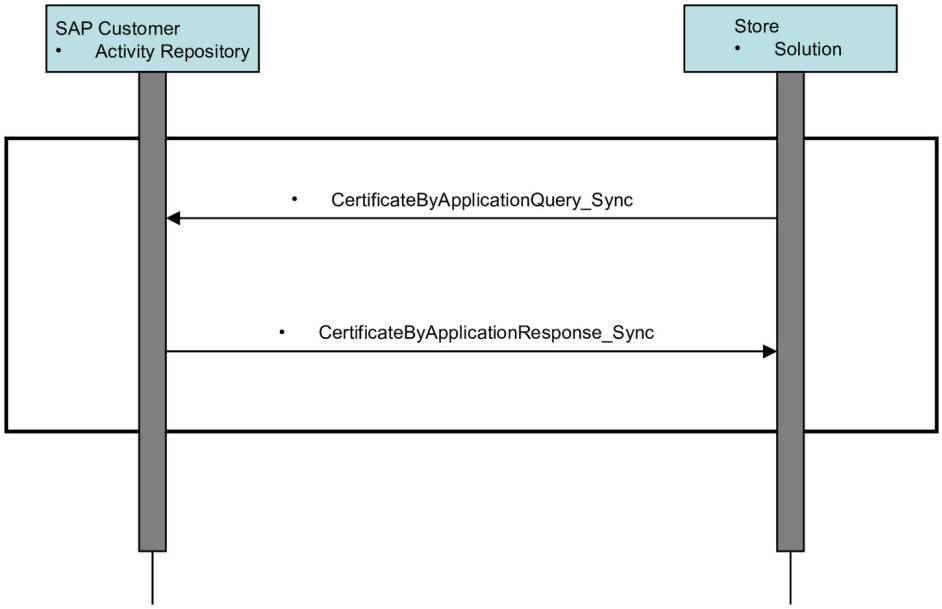



Figure 4: Pull Mechanism

## 13.3.3 Message Choreography SAP Customer Activity Repository and POS Store Solution

Certificates sent using Web services have an X.509 format, the standard format for public key certificates.

The Web service has a query/response pattern that contains one service interface for the query and one for the response. These service interfaces are modeled on the SAP NetWeaver PI system (SAP ABA 7.02 and SAP ABA 7.20). SAP NetWeaver PI core and global data types are used as the data types.

### Service Interface

The `CertificateByApplicationQueryResponse_In` service interface, which has a query/response communication pattern, contains the following three messages:

Table 22

| Name | Type | Role | Description |
|---|---|---|---|
| `CertificateByApplicationQuery_sync` | Message Type | Request | Request for the certificate and the application |
| `CertificateByApplicationResponse_sync` | Message Type | Response | Response that contains the certificate and the version |

| Name | Type | Role | Description |
|---|---|---|---|
| StandardMessageFault | Fault Message Type | Fault | Fault message |

CertificateByApplicationQuery_sync is the message type for the request section of the CertificateByApplicationQueryResponse_In service interface. It contains the SSF application for which the certificate is being requested.

Table 23

| Name | Type | Description |
|---|---|---|
| Application | String | SSF Application |

The CertificateByApplicationResponse_sync message contains the current certificate and version of the requested application.

Table 24

| Name | Type | Description |
|---|---|---|
| Certificate | BinaryObject | X.509 Certificate |
| Version | IntegerValue | Current active version of the certificate |
| Log | Log | GDT Log |

The SSF application is required for the following reasons:

- It is the importing parameter of the SSFV_GET_CURRENT_KEYVERS_RFC function module, which is called from the proxy class.
- Without the SSF application, it is not possible to get the key version.

### Syntax

```
IMPORTING
  VALUE(IF_APPLIC) TYPE  SSFAPPL
EXPORTING
  VALUE(EF_KEYVERSION) TYPE  SSFKEYVERS
  VALUE(EF_CERTIFICATE) TYPE  XSTRING
EXCEPTIONS
    VERSION_NOT_FOUND
    CERTIFICATE_NOT_FOUND
```

The corresponding class of the proxy contains a method with an importing parameter that is the request message type and an exporting parameter that corresponds to the response message type.

## SAP Customer Activity Repository Keys

Key rotation in SAP Customer Activity Repository is performed using the STRUST transaction. SAP Customer Activity Repository also provides you with a key management tool. The /POSDW/KEY_DISTRIB_DISPLAY report displays information about used and distributed key versions.

### Recommendation

The key management tool performs a selection on a large central log database that can be used by many applications, therefore you must make the selection as specific to your needs as possible. For example, select the following:

- Application log object: KEY_DIST
- SSF application: PAYCRV

The results of the selection allow you to identify:

- Any key versions activated for deletion
- The key versions still in use
- The system to which the key was distributed

## 13.3.4 Key Distribution User Interface

The /POSDW/DISP_KEYV transaction displays a list of the key versions and allows you to do the following:

- Track which users required a key
- Link to the transaction where an administrator can perform key management
- Flag a key version for deletion. This requires a manual verification by the administrator to ensure that there are no inbound messages using the encrypted key that is flagged for deletion.

### Customizing

At least one key version must exist. An administrator can create key versions using the SSFVA transaction.

### Process

Every time the user uses the Key Distribution Web service, the information is saved in the application log. The key version is written in a message structure of the log. The user name, date, time, KEY_DISTR application log object, SSFV application name, transaction and log number are also written to the log.

An administrator can run the /POSDW/KEY_DISTRIB_DISPLAY report to search the application log and display information. The existing backend capacity of the application log provides search functionality, persistence of data and retrieval functionality from the database. The displayed information is read-only.

After the administrator manually verifies in the POS, SAP NetWeaver PI, and SAP Customer Activity Repository to ensure that they do not contain encrypted information with a particular key version, the administrator can flag this key version for deletion using the corresponding button (under the description FLG_DEL). The rest of the deletion process can be carried out by choosing the KEY_MGNT button to execute the SSFVA transaction.

## 13.4 Masked/Unmasked Display

The payment card security settings, described in the PCI-Related Customizing [page 51] section, specify the following:

- Security level - with or without encryption/masking
- Update of the access log with unmasked display
- Selection of additional authorization check with unmasked display
- Number of unmasked characters displayed

In SAP Customer Activity Repository, credit card numbers can only be displayed in the POS Workbench (using the /POSDW/MON0 transaction). When a user displays the details of a sales transaction with a means of payment

that includes a credit card settlement segment, the credit card details are masked (that is, an asterisk (*) is used to replace each number). If the B_CCSEC authorization object exists in the user's master record, the user has the authorization level required to display the credit card details in an unmasked form. The user can display the credit card details using the magnifier icon next to the credit card number. This action triggers a new entry in the access log and opens a new window that displays the unmasked details.

The logging mechanism allows you to trace which user has displayed which payment card and when. If the user does not have the authorization level required to display unmasked credit card numbers, the magnifier icon is not displayed in the POS Workbench.

> **Caution**
>
> In order for a user to be able to view any credit card information in the POS Workbench, you must enable the W_POS_CCNR authorization object for activity 02, Display Credit Card Number.

The SAP Basis authorization role B_CCARD is enhanced to allow the display of unmasked credit card data.

The /POSDW/SALES_AUDIT authorization role allows auditors to review credit card settlement information.

At a minimum, the following credit card data fields must be encrypted:

- Credit card expiration date
- Credit card holder name
- Authorization number
- Credit card number

The W_POS_FSPR authorization object specifies the protection level required for this sensitive data. The authorization object has only one field, *Field Selection Profile*. It is used to specify if data is to be displayed in the interface or not, depending on which profiles are added to it for a specific user or role.

In Customizing for SAP Customer Activity Repository, you can define field selection profiles. This allows you to define what information is displayed for a user profile, that is, which list of structures and fields are visible to a user based on a user's profile.

## 13.5 Logging of Payment Card Number Access

SAP Customer Activity Repository uses the following SAP Basis reports and programs to display and delete logs about user access to unmasked credit card data:

- The CCSEC_LOG_SHOW transaction - allows users to display a log of users who have viewed decrypted credit card information in the POS Workbench. To access the log, a user must have authorization for activity 71 in the B_CCSEC authorization object.
- The CCSEC_LOG_DEL transaction - allows users to delete log records about users who have accessed unmasked credit card data in the POS Workbench. A user can only delete log records that are at least one year old. To activate the deletion program, a user must have authorization for activity 06 in the B_CCSEC authorization object.

> **Note**
>
> The integrity of the log does affect your PCI-DSS compliance. If the log is not secured, your PCI-DSS compliance is compromised.

## 13.6 Encryption, Decryption, and Storage of Encrypted Credit Card Numbers

SAP Customer Activity Repository stores transactional data in the /POSDW/TLOGF table. The table contains the /POSDW/LRAW transactional data, which is stored in a 32000-length LRAW string. This is the only table in SAP Customer Activity Repository in which credit card data is stored. All credit card data stored in the LRAW strings must be encrypted.

### 13.6.1 SAP Customer Activity Repository

#### IDoc Encryption

BAdIs are used to encrypt and decrypt data. The IDOC_DATA_MAPPER BAdI is used to encrypt and save data to the IDoc database. The IDOC_DATA_CRYPTION is used to read and decrypt data from the IDoc database.

Three IDoc types contain credit card numbers:

- WPUBON01
- WPUTAB01
- /POSDW/POSTR_CREATEMULTIPLE02

The /POSDW/PCA_IDOC_MAP BAdI is used to encrypt credit card numbers in the WPUBON01 and WPUTAB01 IDocs. The /POSDW/PCA_IDOC_CRYPT BAdI implementation is used to decrypt credit card numbers in the WPUBON01 and WPUTAB01 IDocs.

To enable the encryption of credit card numbers in the /POSDW/POSTR_CREATEMULTIPLE02 IDoc type, the CARDGUID and ENCTYPE fields have been added to the /POSDW/E1BPCREDITCARD segment of the /POSDW/POSTR_CREATEMULTIPLE02 IDoc basic type. The /POSDW/PCA_IDOC_MAP and /POSDW/PCA_IDOC_CRYPT BAdIs have been enhanced to process the updated segment type.

#### Processing of Incoming Encrypted Data

The /POSDW/BAPI_POSTR_CREATE BAPI, the /POSDW/CREATE_TRANSACTIONS_EXT remote function module and the service inbound interfaces have been enhanced to contain a secured data segment or cipher; they have all been asymmetrically encrypted using PKCS7.

The decrypted secured data must conform to a defined XML structure and is converted to an internal table for later processing by the /POSDW/XSLT_SECUREXMLTOTABLE simple transformation.

### 13.6.2 SAP ERP

#### IDoc Encryption Process

Once the IDoc data records have been sent to the IDOC_PCI_ENCR_IM BAdI implementation, the encryption of the credit card data begins. The encryption process is as follows:

1. The segment in the IDoc record that contains the credit card information is identified.
2. The encryption process maps the data from the E1WPZ02 and E1WPB06 segments to the internal structure.

3. The data is used to retrieve the card GUID, the name of the credit card institution number, and the credit card number.
4. The security level check is performed.

   In Customizing, each credit card institution is assigned a security level. If the security level is set to 2, the credit card number is encrypted; if the security level is set to 1, the credit card number is masked.
5. The card GUID and encryption type are mapped to the structure for decryption.
6. A message is created to confirm the success or failure of the encryption.
7. The consistency check is performed.

### Decryption Process

Once the IDoc data records have been sent to the `IDOC_PCI_DECRYPTION_IM` BAdI implementation, the decryption of credit card data begins. The decryption process is as follows:

1. The segment in the IDoc record that contains the credit card information is identified.
2. The decryption process maps the data from the `E1WPZ02` and `E1WPB06` segments to the internal structure.
3. The data is used to retrieve the card GUID, the encryption type, and the credit card number.

The encryption type is currently a fixed value set to 2.

1. The credit card number is decrypted.
2. A message is created to confirm the success or failure of the decryption.

### Secure Handling of Credit Card Information During POS Processing

In SAP Customer Activity Repository, credit card data is handled during inbound and outbound processing. Inbound and outbound processing are executed using IDoc types.

During outbound processing, store systems are provided with customer-specific credit card master data. Outbound processing is executed using the `WP_PER01` IDoc type. However as this IDoc type is for internal use only, it cannot be used for the encryption of credit card data.

During inbound processing, credit card details are a payment attribute of sales transactions. Encryption is required on the IDoc database to support IDoc types that contain credit card data. No other changes are required to securely handle credit card data:

- No encryption of the customer POS database is required as no business data or credit card data is stored in it.
- Follow-on applications, such as the Retail Information System (RIS) or Business Warehouse (BW), are only provided with masked credit card numbers in order to perform cross-selling analysis, therefore they do not require to support encryption.
- No changes are required to the user interfaces of the POS Monitor or Sales Audit because the behavior remains the same as it was before the IDoc database was encrypted: the credit card information is provided in clear text format. Credit card information is temporarily available in clear text during inbound processing to internal applications and when the data is transferred to follow-on applications (such as Analytics and Sales & Distribution). However, as the risk of losing credit card data at this point is minimal, no changes for encryption are required.
- Only authorized users can see the credit card data; regular users cannot see secure data while it is being processed internally.

## 13.7 Migration

The /POSDW/PCA_MIGRATION report allows you to move decrypted or encrypted credit card numbers from other systems to masked or encrypted credit card numbers in SAP Customer Activity Repository. You can access the /POSDW/PCA_MIGRATION report using the /POSDW/PCAM transaction.

To use the /POSDW/PCA_MIGRATION report, you must have authorization for activity 02 in the W_POS_TRAN authorization object. The required underlying security settings must also be configured.

You can consult the migration log to determine for which transactions the data was not migrated successfully. The log provides an overview, by store and transaction date, of how many transactions were found and whether or not the data was successfully changed. If an error occurred for a transaction, no credit card numbers or information is displayed in the log, only the transaction index, store number, posting date, and task number are provided.

Transaction data can only be changed if it is not posted in any task. All tasks for the transaction must have one of the following statuses:

- Ready
- Error
- Canceled
- Canceled with Warning

Only transaction data that is not posted to a task can be changed. All transactions must have one of the following statuses:

- Ready
- Error
- Canceled
- Canceled with Warning

> **Note**
>
> Only transaction data from a task with a *Completed* status can be changed.

## 13.8 Deletion of Credit Card Storage

You may be required to delete credit card data, for example, if credit card information is outsourced or in order to improve your PCI-DSS compliance. Once TLOG transactional data has been archived, SAP Customer Activity Repository assumes that the old credit card information is no longer accessible and that it will be deleted eventually. The process deleting old credit card information takes approximately two years as the old data is overwritten by the new data.

The RCCSECV_DATA_DEL SAP standard report from the CCSECV_DATA_DEL transaction allows you to delete unused, encrypted credit card data. By default, credit card data is considered unused when it has not been used in a report or transaction for a minimum of 500 days.

If you have any existing transactions that contain credit card information without an assigned security level, you can use the /POSDW/PCAM transaction to migrate it.

## 13.9 Archiving

Only masked credit card information can be archived. Clear text credit card information must not be archived. Archiving encrypted credit card information is problematic because archived data must remain unchanged. PCI-DSS requires that encrypted credit card information be re-encrypted with a different key, for example, with key rotation. However, it is not possible to change data in this way in an archive.

Archiving must be disabled on applications and transactions that do not retain the encryption state of the source data, such as on SAP NetWeaver PI, ABAP Web Services, or Forward Error Handling (FEH). IDocs that contain credit card information must not be archived. The following IDocs are affected because they may contain credit card information:

- `WPUBON` - POS interface: Upload sales docs (receipts) non-aggregated
- `WPUTAB`- POS interface: Upload day-end closing POS
- `WPUFIB` - POS interface: Upload Fin.Acc. interface SRS/POS
- `/POSDW/POSTR_CREATEMULTIPLE` - PIPE: BAPI for Creating Several POS Transactions

You use the `CA_PCA_SEC` archiving object to archive the encrypted credit card numbers.

You use the following object to archive TLOG transaction data (which may also contain credit card information):

- `/POSDW/TLF`

## 13.10 Interfaces for IDoc/Services

In a typical SAP Customer Activity Repository landscape, credit card information is communicated as follows:

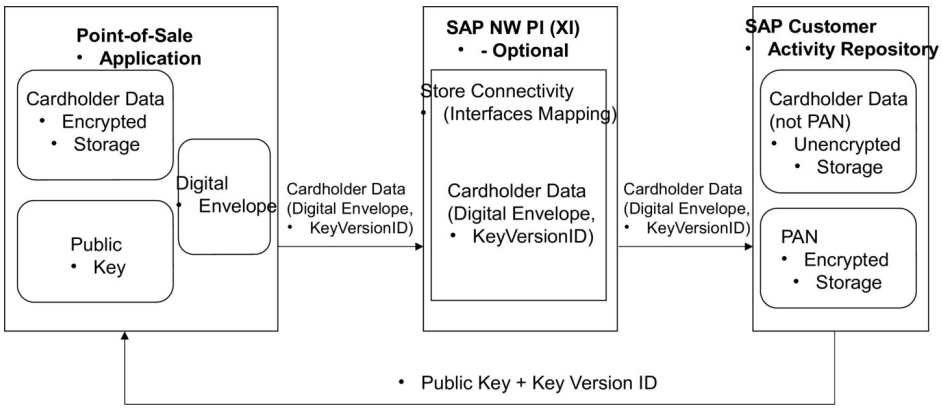



Figure 5: Credit Card Information Communication Flow

See the Credit Card Usage Overview [page 49] section for more information.

The following interfaces are available for use:

- Web services `CertificateByApplicationQuery_Sync` and `CertificateByApplicationResponse_Sync` are used as a pull mechanism from SAP Customer Activity Repository.
- Store Connectivity 2.0 or 3.0 can optionally be used to map the encrypted data container to the SAP Customer Activity Repository inbound proxy.

The interface determinations must contain the `POSLog_To_PointOfSaleTransactionERPBulkCreateRequest_In` interface mapping

- The `IDOC_DATA_MAPPER` IDoc for database encryption is called before saving data to the IDoc database and `IDOC_DATA_CRYPTION` IDoc for database decryption is called after reading data from the database.
- The `POSDW/BAPI_POSTR_CREATE`BAPI, the `/POSDW/CREATE_TRANSACTIONS_EXT` remote Function Module and the service inbound interfaces have been enhanced to contain a secured data segment or cipher; they have all been asymmetrically encrypted with PKCS7. The decrypted secured data must conform to a defined XML structure and is converted to an internal table for processing later by the `/POSDW/XSLT_SECUREXMLTOTABLE` transformation.

The following IDoc types contain credit card numbers:

- `WPUBON01`:

  Encryption in BAdI function `/POSDW/PCA_IDOC_MAP`
- `WPUTAB01`:

  Encryption in BAdI function `/POSDW/PCA_IDOC_CRYPT`
- `/POSDW/POSTR_CREATEMULTIPLE02`:

  To enable the encryption of the credit card number in the IDoc type, the `CARDGUID` and `ENCTYPE`fields have been added to the `/POSDW/E1BPCREDITCARD` segment of the IDoc basic type.

> **Caution**
>
> IDoc segments cannot store credit card numbers in clear text due to the PCI-DSS compliance. Once an IDoc is being processed within the IDoc Framework, all values are temporarily stored, including the credit card number in clear text format.

For more information about how to process IDocs that contain credit card information, see *Handling Sensitive Data in IDocs* in the SAP NetWeaver *Security Guide ALE (ALE Applications)* .

## 13.11 RFC Debugging

You must disable RFC debugging when you process credit card information in a productive system. Do not activate the *Set RFC Trace* option in your productive system. If this option is activated, the system will save all RFC call input data in clear text to file. If credit card numbers (including the PAN) are included in calls to a function module, then this data would be stored to the same file. According to PCI-DSS, credit card numbers must be encrypted when stored, therefore if you activate the *Set RFC Trace* option you would no longer be PCI-DSS compliant.

## 13.12 Forward Error Handling

In SAP Customizing, you must disable Forward Error Handling (FEH) for all services that contain credit card numbers.

## 13.13 Card Verification Values

You must not process any asynchronous services that contain a card verification code or card verification value (CVV) data (such as CAV2, CID, CVC2, CVV2). The payload of asynchronous services is persisted in the database until the service is processed, however, PCI-DSS does not allow the persistence of card verification values. Synchronous services can be processed because their payload is not persisted.

> **Note**
>
> In SAP services, these values correspond to the `PaymentCardVerificationValueText` SAP Global Data Type (GDT).

# 14 Security-Relevant Logging and Tracing

SAP Customer Activity Repository relies on the logging and tracing mechanisms of SAP NetWeaver.

For more information on tracing and logging, see *Auditing and Logging* in the *SAP NetWeaver Security Guide*.

The SAP Customer Activity Repository application (and specifically the POS Data Management component) delivers and uses `/POSDW/PIPE`, an SAP NetWeaver Application Server ABAP application log object for application log entries. This object contains the following subobjects:

- `CHANGE_TASKSTATUS`: Used for task status change related operations
- `CREATETREX`: Used for TREX index-related operations
- `CREDITCARD_MIGRATION`: Used for credit card migration operations
- `DELETE`: Used for operations related to transaction deletion
- `DELETE_AGGREGATE`: Used for operations related to transaction aggregate deletion
- `IDOC_DISPATCHER`: Used for the execution of IDoc Dispatcher processing
- `INBOUND_DISPATCHER`: Used for the executions of Inbound Processing Dispatcher using Queue
- `OUTBOUND_DISPATCHER`: Used for execution of Outbound Processing of Aggregates
- `PIPEDISPATCHER`: Used for execution of PIPE/POS Dispatcher processing
- `REFRESH_INDEX`: Used for operations related to reconstruction of the transaction index
- `REORG_TIBQ`: Used for operations related to the reorganization of the inbound queue for point-of-sales transactions (TIBQ)
- `STOREDAYCHANGE`: Used for operations related to POS Data Key Changes
- `XML_IN`: Used for execution of the Import POS Transaction as XML File
- `XML_OUT`: Used for execution of the Export POS Transaction as XML File

## Logging and Tracing for Customizing Changes

To evaluate changes the individual SAP Customer Activity Repository Customizing tables, you can activate the logging of changes to table data:

1. Use transaction **SE13** to change the technical settings of the desired table and activate the logging of changes.
2. Use transaction **SCU3** to evaluate the generated logs.

## Logging of Payment Card Number Display

SAP Customer Activity Repository users with the appropriate authorization (`B_CCSEC` authorization object) can view complete credit card numbers in clear text in the POS Workbench. When a user displays a payment card number in clear-text format, SAP Customer Activity Repository logs it in an access log. SAP Customer Activity Repository allows you to perform a trace to determine which user has displayed a particular card number and when. You can make changes to the authorization log using one of the following programs:

Table 25

| Program | Description | Prerequisite |
|---|---|---|
| CCSEC_LOG_SHOW | Allows you to evaluate the access to payment card data | Authorization for activity 71 in the B_CCSEC authorization object |
| RCCSEC_LOG_DEL | Allows you to delete log records that are more than one year old | Authorization for activity 06 in the B_CCSEC authorization object |

# 15 Services for Security Lifecycle Management

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

### Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.

  In this case, analyze and implement the identified SAP Notes if possible. If you cannot implement the SAP Notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified.

  In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.
- Whether standard users with default passwords have been identified on your system.

  In this case, change the corresponding passwords to non-default values.

### Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security-relevant configuration parameters
- Critical users
- Missing security patches

This service is available as a self-service within SAP Solution Manager, as a remote service, or as an on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation for a system audit.

### Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users do not have default passwords.

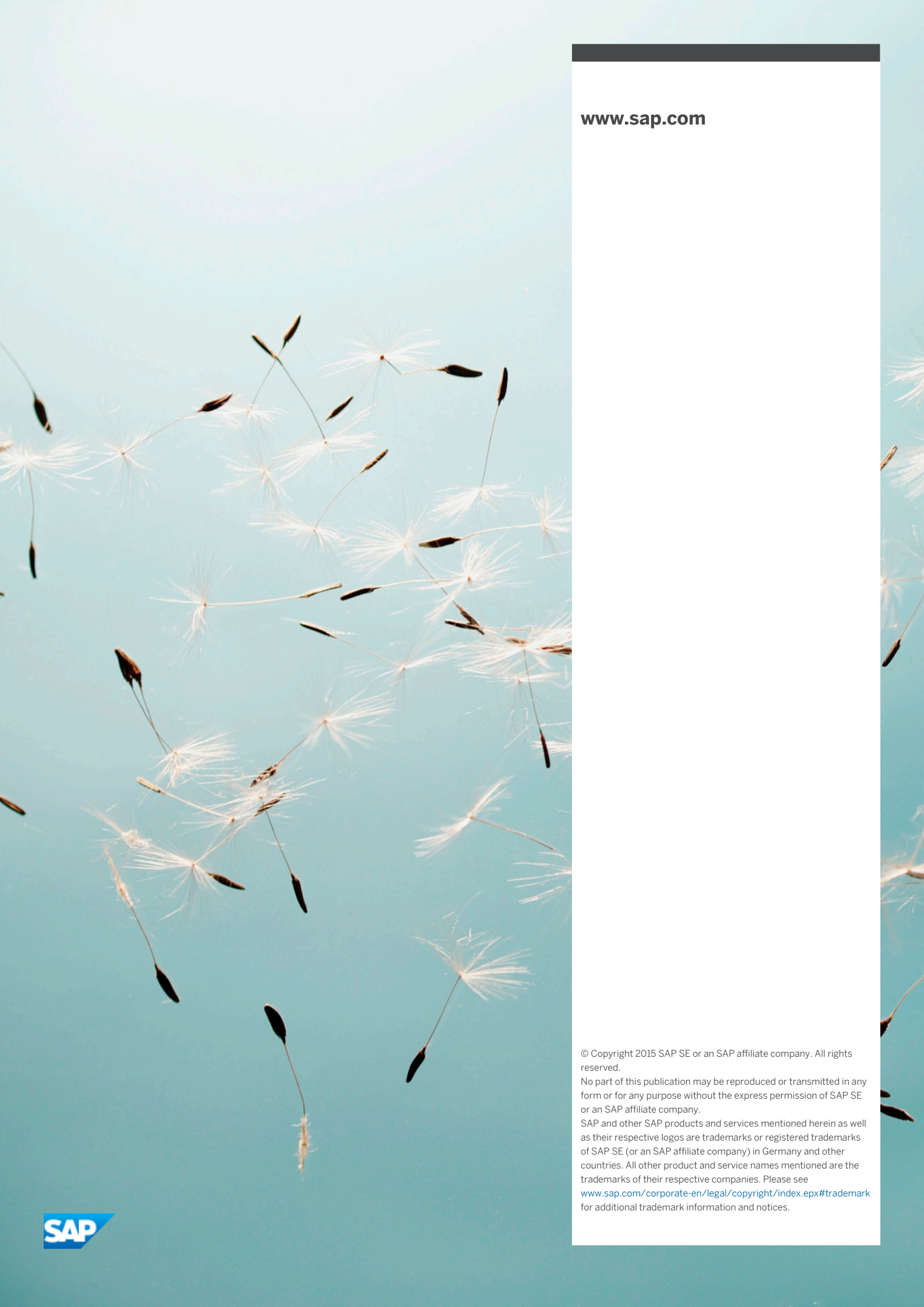
### Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in a secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

## More Information

For more information about these services, see:

- EarlyWatch Alert: service.sap.com/ewa
- Security Optimization Service / Security Notes Report: service.sap.com/sos
- Comprehensive list of Security Notes: service.sap.com/securitynotes
- Configuration Validation: service.sap.com/changecontrol
- RunSAP Roadmap, including the Security and the Secure Operations Standard: service.sap.com/runsap
  (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)



**www.sap.com**